



Dwadzieścia Najbardziej Krytycznych Internetowych Luk Bezpieczeństwa

Wersja 5.0, 8 października 2004 Copyright (C) 2001-2004, SANS Institute

Pytania/komentarze prosimy kierować na top20@sans.org.

----- [Przejdź do indeksu najczęstszych zagrożeń](#) -----

Wprowadzenie

Lista Top 20 Internetowych Luk Bezpieczeństwa według SANS

Większość przypadków propagacji robaków i innych udanych ataków sieciowych jest możliwa, ze względu na luki w kilku popularnych usługach sieciowych systemów operacyjnych. Atakujący są oportunistami. Wybierają najłatwiejszą i najwygodniejszą drogę i wykorzystują najbardziej znane luki, za pomocą najskuteczniejszych i najpowszechniejszych narzędzi. Liczą na to, że organizacje podłączone do sieci nie zadbają o załatwienie znanych błędów. Najczęściej atakują kogo się da, skanując Internet w celu wyszukania podatnych systemów. Szybka i destrukcyjna propagacja robaków, takich jak Blaster, Slammer i Code Red, wynika ze skutecznego wykorzystania niezalutanych luk.

Cztery lata temu SANS Institute wspólnie z FBI w postaci amerykańskiego National Infrastructure Protection Center (NIPC) opublikowały listę Dziesięciu Najbardziej Krytycznych Internetowych Luk Bezpieczeństwa - *Ten Most Critical Internet Security Vulnerabilities*. Tysiące organizacji wykorzystało tę listę oraz późniejsze listy Top 20 (opublikowane rok oraz dwa lata później) do spriorytetyzowania celów pod kątem zamknięcia najbardziej istotnych luk. Na liście znajdują się usługi, których luki doprowadziły do szybkiej propagacji robaków Blaster, Slammer, Code Red oraz NIMDA.

Obecna uaktualniona lista SANS Top 20 składa się tak naprawdę z dwóch list Top 10: dziesięć najczęściej wykorzystywanych podatności w usługach systemów Windows oraz dziesięć najczęściej wykorzystywanych podatności w usługach systemów UNIX i Linux. Choć w sieci rokrocznie mamy do czynienia z tysiącami incydentów naruszenia bezpieczeństwa, związanymi z tymi systemami operacyjnymi, znacząca większość udanych ataków korzysta z jednej lub kilku z opisanych 20 podatnych usług.

Lista Top 20 jest listą luk, które wymagają natychmiastowej naprawy. Jest rezultatem procesu, w którym brało udział wielu czołowych ekspertów od bezpieczeństwa. Specjaliści wywodzili się z najbardziej wyczulonych na tematykę bezpieczeństwa agencji federalnych USA, Anglii i Singapuru, a także z wiodących producentów systemów i rozwiązań bezpieczeństwa oraz firm konsultingowych, czołowych akademickich programów bezpieczeństwa, wielu organizacji zrzeszających użytkowników tych systemów oraz z SANS Institute. Lista uczestników dołączona jest na końcu tego dokumentu.

SANS Top 20 jest dokumentem stale aktualizowanym. Zawiera dokładne instrukcje postępowania oraz wskazówki pozwalające uzyskać dodatkowe informacje, jak naprawić błędy bezpieczeństwa. Będziemy uaktualniać listę oraz instrukcje w miarę identyfikacji nowych zagrożeń oraz nowszych lub wygodniejszych metod zabezpieczeń.

Chętnie skorzystamy także z Twoich uwag. Dokument ten oparty został na konsensusie środowiska. Twoje doświadczenie w walce z włamywaczami i usuwaniu luk może pomóc innym. Sugestie prosimy wysyłać na adres top20@sans.org.

Uwagi dla Czytelników

Wpisy CVE

W dokumencie znajdziesz odwołania do wpisów CVE (Common Vulnerabilities and Exposures) dla każdej luki. Mogą się także zdarzyć wpisy CAN. Wpisy CAN oznaczają kandydatów na wpisy CVE. Wpisy CAN nie zostały poddane pełnej weryfikacji. Aby uzyskać więcej informacji na temat projektu CVE, zobacz <http://cve.mitre.org/>.

Wpisy CVE i CAN odzwierciedlają najistotniejsze podatności, które powinny zostać zweryfikowane dla każdej pozycji na liście. Każdy odnośnik CVE jest skojarzony z serwisem indeksującym ICAT amerykańskiego National Institute of Standards and Technology (<http://icat.nist.gov/>). ICAT zawiera krótki opis każdej luki, jej cech charakterystycznych (np.:zakres ataków i potencjalny rezultat), listę podatnego oprogramowania i ich wersji, a także linki do zaleceń i informacji o aktualizacjach.

Porty do zablokowania na firewallu

----- [Przejdź do listy portów do zablokowania na firewallu lub gatewayu](#) -----

Na końcu dokumentu możesz znaleźć dodatkową sekcję, w której jest sprecyzowana lista często skanowanych i atakowanych portów. Blokada tych portów na firewallach lub poprzez inne techniki zabezpieczające styk ze światem zewnętrznym, może stworzyć dodatkową warstwę zabezpieczeń, która uchroni sieć na wypadek błędów konfiguracji oraz zaniedbań. Należy jednak pamiętać, że wykorzystanie firewalla lub routerów do zablokowania portu nie ochroni sieci przed niezadowolonymi współpracownikami wewnątrz sieci oraz przed hakerami, którzy spenetrowali sieć innymi metodami. Należy też podkreślić, że znacznie bezpieczniejszym podejściem jest zaimplementowanie polityki domyślnego blokowania wszystkiego na firewallach i routerach, i odblokowania wyłącznie niezbędnych usług, zamiast blokowania tylko wybranych portów.

[przejdź do początku dokumentu](#) ^

Najczęstsze luki w systemach Windows

- [W1 Serwery i usługi WWW](#)
- [W2 Usługa stacji roboczej](#)
- [W3 Usługi zdalnego dostępu w Windows](#)
- [W4 Serwer Microsoft SQL \(MSSQL\)](#)
- [W5 Uwierztałnienie w Windows](#)
- [W6 Przeglądarki WWW](#)
- [W7 Aplikacje wymiany plików](#)
- [W8 LSASS](#)
- [W9 Klient poczty elektronicznej](#)
- [W10 Komunikatory IM](#)

Najczęstsze luki w systemach UNIX

- [U1 Serwer nazw BIND](#)
- [U2 Serwer WWW](#)

- U3 Systemy kontroli wersji
- U4 Uwierzytelnienie
- U5 Serwer pocztowy (MTA)
- U6 Simple Network Management Protocol (SNMP)
- U7 Open Secure Sockets Layers (SSL)
- U8 Błędy w konfiguracji NIS/NFS
- U9 Bazy danych
- U10 Jądro

[przejdź do początku dokumentu ^](#)

Najczęstsze luki w systemach Windows (W)

W1 Serwery i usługi WWW

W1.1 Opis

Domyślne instalacje różnych serwerów WWW oraz innych składników obsługujących zapytania HTTP i transmisję strumieniową okazały się podatna na kilka poważnych ataków. Ataki te mogą grozić między innymi:

- Zablokowaniem świadczenia usług (atak Denial of Service)
- Ujawnieniem zawartości lub modyfikacją wrażliwych plików lub danych
- Wykonaniem dowolnych komend na serwerze
- Całkowitym przejęciem serwera

Serwery HTTP, takie jak IIS, Apache czy iPlanet (obecnie SunOn) były dotknięte różnymi słabościami, naprawianymi w miarę ich odkrywania. Należy się upewnić, że na serwerze działa aktualna wersja oprogramowania oraz zainstalowane są wszelkie dostępne poprawki. W przypadku większości serwerów HTTP ich domyślna konfiguracja jest dość otwarta, pozostawiając szerokie pole do wykorzystania przez atakującego. Należy więc poświęcić nieco czasu na tak modyfikacje konfiguracji, które pozwolą na zapewnienie jedynie minimalnej funkcjonalności niezbędnej do prawidłowego funkcjonowania serwera.

IIS używa mechanizmu tzw. ISAPI do kojarzenia pewnych rozszerzeń z bibliotekami DLL (zwanymi filtrami ISAPI). Preprocesory takie jak ColdFusion czy PHP także używają ISAPI, a IIS zawiera wiele filtrów ISAPI, realizujących między innymi funkcje Active Server Pages (ASP), usługi sieciowe .Net oraz współdzielenia drukarek w sieci. Wiele filtrów ISAPI instalowanych domyślnie wraz z IIS nie jest niezbędnych do poprawnej pracy w większości instalacji. Wiele z nich jest natomiast podatnych na ataki. Przykładami wykorzystania luk w IIS jako mechanizmu propagacji złośliwego kodu są robaki Code Red i Code Red 2. Należy włączyć jedynie te rozszerzenia ISAPI, które muszą być wykorzystywane przez serwer. Zaleca się także ograniczenie opcji HTTP możliwych do użycia z każdym z rozszerzeń.

Większość serwerów WWW zawiera przykładowe strony aplikacji, których celem jest demonstracja funkcjonalności serwera. Nie zostały one zaprojektowane do bezpiecznego działania w środowisku produkcyjnym. Niektóre przykładowe aplikacje serwera IIS pozwalały na zdalne przeglądanie i nadpisywanie wybranych plików, a także zdalny dostęp do niektórych wrażliwych informacji o serwerze – w tym do hasła administratora. Należy usunąć takie aplikacje przed umieszczeniem serwera w środowisku produkcyjnym.

Instalacja IIS pozbawiona regularnego dozoru będzie także zawierać luki, które wykryto od momentu publikacji oprogramowania. Przykładem mogą być luki w PCT i SSL, których dotyczy poprawka MS04-011, a które pozwalały na zablokowanie działania serwera lub przejęcie przez atakującego pełnej kontroli nad nim. Z tych powodów instalacja dostępnych poprawek w jak najkrótszym czasie, w szczególności na publicznie dostępnych serwerach WWW, jest sprawą krytyczną.

Dodatki firm trzecich, takie jak ColdFusion czy PHP, mogą wprowadzić do systemu z serwerem IIS kolejne podatności. Mogą one być efektem zarówno nieprawidłowej konfiguracji, jak i luk w samym produkcie.

W1.2 Podatne systemy operacyjne

Problemy mogą dotyczyć każdego systemu z zainstalowanym serwerem WWW. W szczególności (lecz nie wyłącznie) dotyczy:

- Microsoft IIS: Windows NT 4.0 i nowsze, w tym Windows XP Professional
- Serwer HTTP Apache: wspierany na Windows NT 4.0 SP3 i nowszych; może działać także na Windows 95/98
- Sun Java System/Sun One/iPlanet Web Server: Windows NT 4.0 SP6 i nowsze

Uwaga: Windows 2000 Server zawiera w domyślnej instalacji serwer IIS. Wielu administratorów przekonało się o tym w następstwie niesławnych epidemii Code Red i Nimdy. Ponadto, wiele aplikacji wymaga funkcjonalności dostarczanej przez IIS, co może skutkować instalacją tego serwera wraz z taką aplikacją, być może bez świadomości administratora. Nie należy nigdy zakładać, że opisane problemy nie dotyczą danej sieci jedynie dlatego, że nie został w niej świadomie zainstalowany żaden ze wspomnianych serwerów. Należy regularnie sprawdzać sieć na okoliczność występowania serwerów, które nie powinny znajdować się w sieci.

W1.3 Wpisy CVE/CAN

a. IIS

[CVE entries for IIS 2.0](#)
[CVE entries for IIS 3.0](#)
[CVE entries for IIS 4.0](#)
[CVE entries for IIS 5.0](#)

b. Apache

[CAN-2001-0729](#), [CAN-2002-0249](#), [CAN-2002-0654](#), [CAN-2002-0661](#), [CAN-2002-0661](#), [CAN-2003-0016](#), [CAN-2003-0017](#), [CAN-2003-0460](#), [CAN-2003-0844](#), [CAN-2004-0492](#), [CAN-2004-0493](#)

[CVE-1999-0448](#), [CVE-2000-0505](#), [CVE-2001-1342](#), [CVE-2001-1342](#)

Moduły serwera Apache: [CAN-2003-0844](#), [CAN-2004-0492](#)

c. iPlanet/Sun

[CAN-2002-0686](#), [CAN-2002-1042](#), [CAN-2002-1315](#), [CAN-2002-1315](#), [CAN-2002-1316](#),
[CAN-2003-0411](#), [CAN-2003-0412](#), [CAN-2003-0414](#), [CAN-2003-0676](#), [CAN-2003-0676](#)

[CVE-2000-1077](#), [CVE-2000-1077](#), [CVE-2001-0252](#), [CVE-2001-0327](#), [CVE-2001-0327](#),
[CVE-2002-0845](#), [CVE-2002-0845](#)

d. Dodatki

[CAN-1999-0455](#), [CAN-1999-0477](#), [CAN-1999-1124](#), [CAN-2001-0535](#), [CAN-2001-1120](#),
[CAN-2002-1309](#), [CAN-2003-0172](#)

[CVE-1999-0756](#), [CVE-1999-0922](#), [CVE-1999-0924](#), [CVE-2000-0410](#), [CVE-2000-0538](#)

ColdFusion: [CVE-1999-0756](#), [CVE-1999-0760](#), [CVE-1999-0922](#), [CVE-1999-0924](#),
[CAN-2002-1309](#), [CAN-2004-0407](#), [CVE-2000-0189](#), [CVE-2000-0382](#), [CVE-2000-0410](#),
[CVE-2000-0538](#), [CVE-2002-0576](#)

PHP: [CAN-2002-0249](#), [CAN-2003-0172](#)

e. Inne usługi

[CAN-1999-1369](#), [CAN-2003-0227](#), [CAN-2003-0349](#), [CAN-2003-0725](#), [CAN-2003-0905](#)

[CVE-1999-0896](#), [CVE-1999-1045](#), [CVE-2000-0211](#), [CVE-2000-0272](#), [CVE-2000-0474](#),
[CVE-2000-1181](#), [CVE-2001-0083](#)

eEye SecureIIS: [CAN-2001-0524](#)

Jakarta Tomcat: [CAN-2003-0045](#)

W1.4 Jak sprawdzić czy Twój system jest podatny na atak?

Każdą instalację serwera WWW wykonaną w sposób domyślny lub bez zainstalowanych dodatkowo poprawek należy uznać za podatną na atak.

Większość producentów serwerów WWW i usług udostępnia zasób informacji dotyczących bieżących problemów bezpieczeństwa ich produktów. Wśród nich należy wymienić:

- Serwer HTTP Apache: [Strona główna](#) oraz [Security Report](#)
- [Microsoft TechNet Security Centre](#)
- [Microsoft Internet Information Server \(IIS\) Security Centre](#)
- [Sun Web, Portal, & Directory Servers Download Centre](#)
- [Macromedia Security Zone](#)
- [Real Networks Security Issues](#)
- PHP: [Strona główna](#) i dział [Downloads](#)

Należy także porównywać własne dane o zainstalowanych wersjach oprogramowania serwerów WWW, związanych z nimi usług, a także ich konfiguracji oraz zainstalowanych łat, z informacjami podawanymi przez producentów i z bazą CVE, celem określenia poziomu zagrożenia. Trzeba zdawać sobie sprawę, że wciąż

wykrywane są nowe luki, co powoduje, że dobrym zwyczajem jest stałe konsultowanie aktualnej bazy CVE.

Istnieją zdalne i lokalne narzędzia, omagające administratorom w audycie własnych sieci, np:

- [Nessus](#) (Open-source)
- [SARA](#) (Open-source)
- [Nikto](#) (Open-source)
- [eEye Narzędzia darmowe](#) i [Skanery komercyjne](#)
- [Microsoft Baseline Security Analyzer](#) (dla serwera IIS)

Zaleca się, by korzystać ze zdalnych skanerów w skali całej sieci, a nie jedynie uwzględniając znane serwery, aby umożliwić wykrycie serwerów, o których obecności nie wiadomo.

W1.5 Jak się przed tym chronić?

Dla większości systemów

1. Zainstaluj odpowiednie poprawki dla usług związanych z HTTP, a także dla systemu operacyjnego i innych aplikacji, działających na tej samej maszynie. Po upewnieniu się, że wszystkie aktualne poprawki są zainstalowane, na bieżąco utrzymuj ten stan.
2. Zainstaluj oprogramowanie antywirusowe i IDS typu host-based. Pamiętaj, o ich aktualizacji i częstym przeglądaniu generowanych przez nie logów.
3. Wyłącz zbędne interpretery skryptów i odinstaluj je lub usuń pliki wykonywalne, np: perl, perlscript, vbscript, jscript, javascript, php.
4. Włącz logowanie, jeżeli jest taka możliwość. Logi przeglądaj regularnie, najlepiej korzystając z oprogramowania do ich analizy, podsumowującego zdarzenia i informującego o zdarzeniach nietypowych.
5. Użyj systemu podobnego do syslog aby przechowywać logi systemu operacyjnego i serwera HTTP na innej maszynie w sposób bezpieczny.
6. Usuń lub ogranicz dostęp do narzędzi powszechnie wykorzystywanych przez atakujących w pierwszej fazie ataku oraz do przenoszenia się na inne maszyny, np: tftp(.exe), ftp(.exe), cmd.exe, bash, net.exe, remote.exe, telnet.exe.
7. Ogranicz aplikacje działające na maszynie do serwera HTTP i wspierających go usług.
8. W miarę możliwości, nie uruchamiaj na maszynie z serwerem HTTP domenowego lub podobnego systemu uwierzytelnienia.
9. Bądź świadom i minimalizuj możliwości dostania się do sieci wewnętrznej z serwerów publicznych, np. przez udostępnione zasoby NetBIOS, relacje zaufania czy powiązania baz danych.
10. Używaj innych konwencji w nazewnictwie kont i tworzeniu haseł w systemach wystawionych na świat, niż w sieci wewnętrznej. Przecieki informacji z systemu dostępnego publicznie nie powinien być pomocą przy atakowaniu sieci wewnętrznej.

a. IIS

Zainstalowanie poprawek na serwerze jest koniecznym, lecz nie dostatecznym warunkiem jego zabezpieczenia. W miarę odkrywania nowych podatności w IIS należy na bieżąco instalować kolejne poprawki. Mechanizmy Windows Update i poprawek automatycznych nadają się do wykorzystania w przypadku instalacji na pojedynczym

serwerze. Pomocą w administrowaniu aktualnymi poprawkami zarówno na maszynie lokalnej jak i na zdalnych, służyć może [HFNetChk](http://www.microsoft.com/technet/security/tools/hfnetchk.asp), the Network Security Hotfix Checker. Narzędzie to działa w Windows NT 4, Windows 2000 oraz Windows XP. Aktualną wersję można pobrać ze strony Microsoft:
<http://www.microsoft.com/technet/security/tools/hfnetchk.asp>.

Ponadto, w Czytelni SANS znajduje się przydatny dokument autorstwa Harpala, zatytułowany [Securing a Windows 2000 IIS Web Server – Lessons Learned](#).

Użyj Kreatora blokady programu IIS do hardeningu instalacji

Microsoft stworzył proste narzędzie, mające pomóc w zabezpieczeniu instalacji IIS, nazwane „Kreator blokady programu IIS”. Opis wykorzystania narzędzia znajduje się na stronach Microsoftu:
<http://support.microsoft.com/default.aspx?scid=kb;pl;325864>.

Uruchomienie Kreatora blokady programu IIS w trybie *custom* lub *expert* pozwoli na wykonanie następujących zmian zalecanych dla instalacji IIS:

- Wyłączenie WebDAV (o ile środowisko nie wymaga jego użycia)
- Wyłączenie skojarzeń dla zbędnych rozszerzeń ISAPI (w szczególności .htr, .idq, .ism i .printer)
- Usunięcie aplikacji przykładowych
- Wyłączenie możliwości wykonywania przez serwer komend systemowych powszechnie używanych przy atakach (np. cmd.exe i tftp.exe)

W Czytelni SANS znajduje się dokument [Using Microsoft's IISlockdown tool to protect your IIS Web Server](#), autorstwa Jeffa Wichmana, dotyczący w szczególności Kreatora blokady programu IIS.

Użyj URLScan do filtrowania zapytań HTTP

W wielu przypadkach wykorzystania luk w IIS, m.in. w Code Blue i rodzinie robaków Code Red, użyto złośliwie spreparowanych zapytań HTTP, aby dostać się do standardowo niedostępnych katalogów (atak directory traversal) lub przepelnić bufor w procesie serwera. Filtr URLScan można skonfigurować tak, aby odrzucał takie zapytania zanim system rozpocznie ich przetwarzanie. Aktualna wersja narzędzia została wbudowana w Kreator blokady programu IIS, ale jest także dostępna samodzielnie na stronach Microsoft:
<http://www.microsoft.com/technet/security/tools/urlscan.mspc>.

b. Apache

Kontroli dostępu, ograniczenia dla poszczególnych adresów IP i moduły serwera Apache związane z bezpieczeństwem, a także wielu innych kwestii zostało omówione na stronach [Apache Tutorials](#) page.

Ponadto, w Czytelni SANS, dostępny jest bardzo przydatny dokument [Securing Apache: Step-by-Step](#) Artura Maja, omawiający zabezpieczanie serwera Apache w szczegółach.

c. iPlanet/Sun One

Edmundo Farinas opisuje zabezpieczanie serwera iPlanet w dokumencie [Security Considerations for the iPlanet Enterprise Web Server on Solaris](#), który znaleźć można w Czytelni SANS.

Ponadto, Sun stworzył dokument [Sun ONE Application Server Security Goals](#), opisujący zalecane kroki przy zabezpieczaniu serwera iPlanet/Sun One.

d. Dodatki

Korzystając z dodatków firm trzecich, np.: ColdFusion, PerlIIS czy PHP, należy pamiętać o szukaniu łat i wskazówek dotyczących konfiguracji także na stronach ich producentów. Z oczywistych przyczyn, Microsoft nie umieszcza w Windows Update czy pokrewnych serwisach aktualizacyjnych łat dotyczących oprogramowania firm trzecich.

Informacje dotyczące zabezpieczania ColdFusion znaleźć można w dokumencie [Web Application Security, with a Focus on ColdFusion](#) Josepha Higginsa, w Czytelni SANS.

Także w Czytelni SANS znajduje się dokument [Securing PHP: Step-by-step](#) Artura Maja, ilustrujący proces zabezpieczania aplikacji napisanych w PHP.

Ponadto, bardzo przydatnym źródłem wiedzy jest [16. rozdział podręcznika PHP \(Security\)](#), opisujący w szczegółach zagadnienia związane z bezpieczeństwem PHP.

e. Inne usługi

Mimo, że istnieje wiele, opisanych powyżej, sposobów, pozwalających na zabezpieczenie większości usług związanych z WWW, każda z nich ma też swoje własne zbiory poprawek, uaktualnień, zalecanych konfiguracji i możliwości rejestracji zdarzeń.

Przejrzyj dokumentację, włączając w to wszelkie informacje udostępniane przez producenta na swojej stronie, a także zapisz się na listy dystrybucyjne, biuletyny itp. oferowane przez producenta, w których mogą być zamieszczane informacje dotyczące bezpieczeństwa. W ten sposób odpowiednio szybko zostaniesz poinformowany o zagrożeniu i będziesz miał możliwość szybkiego i skutecznego podjęcia działań zaradczych.

[przejdź do początku dokumentu ^](#)

W2 Usługa stacji roboczej

W2.1 Opis

Usługa stacji roboczej jest odpowiedzialna za realizację dostępu użytkownika do zasobów takich jak pliki i drukarki. Usługa rozpoznaje, czy żądany zasób znajduje się w systemie lokalnym, czy udostępnionym zdalnie i odpowiednio przekierowuje zapytanie.

Funkcje zarządzania siecią udostępniane przez tę usługę mogą być wywoływane na jeden z poniższych sposobów:

- Wywołania DCE/RPC przez protokół SMB po podłączeniu do usługi potokiem \\pipe\wkssvc.

- Wywołania DCE/RPC bezpośrednio przez port UDP (> 1024).
- Wywołania DCE/RPC bezpośrednio przez port TCP (> 1024).

Usługa zostaje przypisana do pierwszego dostępnego portu TCP i UDP ponad 1024.

Usługa stacji roboczej zawiera lukę przepełnienia bufora związaną ze stosem. Może ona być wykorzystana przez odpowiednio spreparowane wywołanie DCE/RPC. Problem wynika z przyjmowania parametrów przekazywanych do funkcji logującej bez wykonywania sprawdzenia ich wielkości. Korzystając z luki, nieuwierzytelniony atakujący może zdalnie wykonać dowolny kod w podatnym systemie z przywilejami użytkownika System. W ten sposób może doprowadzić do przejęcia całkowitej kontroli nad systemem. Kod wykorzystujący lukę został publicznie umieszczony w Internecie i wykorzystany w niektórych wariantach robaka Phatbot/Gaobot, który zainfekował miliony systemów na całym świecie.

W2.2 Podatne systemy operacyjne

Windows 2000 SP2, SP3 i SP4

Windows XP

Windows XP 64 Bit Edition

W2.3 Wpisy CVE/CAN

[CAN-2003-0812](#)

W2.4 Jak sprawdzić czy Twój system jest podatny na atak?

Maszyny z systemem Windows 2000, w którym nie zainstalowano poprawki MS03-049 oraz Windows XP, w którym nie zainstalowano poprawki MS03-043 są podatne.

Należy sprawdzić następujące wpisy w rejestrze:

KB828035 w kluczu HKLM\Software\Microsoft\Updates\Windows XP (w Windows XP)

KB828749 w kluczu HKLM\Software\Microsoft\Updates\Windows 2000 (w Windows 2000)

Jeżeli wpisy te nie występują, system jest podatny.

Można także skorzystać ze skanera sieciowego, np. Microsoft Baseline Security Analyzer (MBSA) aby sprawdzić, czy odpowiednia poprawka została zainstalowana. MBSA można pobrać ze strony

<http://www.microsoft.com/technet/security/tools/mbsahome.msp>.

W2.5 Jak się przed tym chronić?

1. Upewnij się, że w systemie zainstalowane są wszystkie poprawki związane z bezpieczeństwem. W szczególności, upewnij się, że zainstalowana została poprawka MS03-049 w systemie Windows 2000 lub MS03-043 w systemie Windows XP.
2. Zablokuj porty 139/TCP oraz 445/TCP na brzegach swojej sieci. To przeszkodzi atakującemu w wykorzystaniu przepełnienia bufora przez SMB.
3. Otwórz jedynie niezbędne porty powyżej 1024 na styku z siecią. To przeszkodzi atakującemu w wykorzystaniu przepełnienia bufora przez wywołania DCE/RPC. Zwróć uwagę, że filtrowanie portów UDP powyżej 1024 na firewallu jest skomplikowane, gdyż są one wykorzystywane jako porty tymczasowe.
4. Użyj filtrowania TCP/IP, dostępnego zarówno w Windows 2000 jak i XP lub Zapory połączenia internetowego w Windows XP aby zablokować ruch przychodzący na porty związane z zagrożoną usługą.
5. W przypadku produktów firm trzecich, działających na zmodyfikowanej platformie Windows 2000/XP, zainstaluj odpowiednie poprawki dostarczone

przez producenta. Na przykład, Cisco Systems wydało zalecenie, w którym poinformowano, że kilka produktów Cisco jest podatnych na opisana lukę. Cisco wydało też odpowiednie poprawki.

6. Jeżeli system działa samodzielnie, tzn. nie należy do otoczenia sieciowego Windows, usługa stacji roboczej może zostać wyłączona bez żadnych następstw.

Dodatkowe informacje:

Biuletyn Microsoft

<http://www.microsoft.com/technet/security/bulletin/MS03-049.msp>

Zalecenie eEye

<http://www.eeye.com/html/Research/Advisories/AD20031111.html>

Zalecenia CERT

<http://www.cert.org/advisories/CA-2003-28.html>

<http://www.kb.cert.org/vuls/id/567620>

Zalecenie CORE Security

<http://archives.neohapsis.com/archives/vulnwatch/2003-q4/0066.html>

Zalecenie Cisco

<http://www.cisco.com/warp/public/707/cisco-sa-20040129-ms03-049.shtml>

Gaobot Worm

<http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html>

[przejdź do początku dokumentu ^](#)

W3 Usługi zdalnego dostępu w Windows

W3.1 Opis

Rodzina systemów operacyjnych Windows wspiera rozmaite mechanizmy i technologie sieciowe. Posiada wbudowane wsparcie dla większości standardowych protokołów sieciowych oraz całej gamy rozwiązań specyficznych dla Microsoft. Pośród tych ostatnich znajduje się kilka notorycznie niebezpiecznych i źle konfigurowanych. Należy wśród nich wymienić współdzielone zasoby NetBIOS, anonimowe logowanie przez sesję zerową, zdalny dostęp do rejestru i zdalne wywoływanie procedur (rpc). Stanowią one łącznie znaczny udział w ogólnie rozumianych podatnościach w Windows, wykorzystywanych z poziomu sieciowego i są opisane w poniższym tekście.

NETBIOS – Niezabezpieczone współdzielone zasoby Windows

Microsoft Windows zapewnia komputerowi możliwość udostępniania plików i folderów przez sieć. Funkcjonalność ta oparta jest na protokole Server Message Block (SMB) lub Common Internet File System (CIFS). Oba protokoły pozwalają stacji zdalnej na działanie na plikach i folderach w taki sam sposób, jakby były one dostępne lokalnie. Mimo, że jest to bardzo potężna i użyteczna cecha Windows, nieprawidłowa konfiguracja udostępniania zasobów może zagrozić ujawnieniem krytycznych plików systemowych albo nawet przejęciem kontroli nad maszyną przez obcą osobę lub program. Jednym ze sposobów, które zagwarantowały robakom takim jak I-Worm.Klez.a-h ([Klez Family](#)), Sircam ([CERT Advisory 2001-22](#)) i Nimda ([CERT Advisory 2001-26](#)) szybkie rozprzestrzenienie się w 2001 roku, było wykrywanie niezabezpieczonych udostępnionych folderów i umieszczanie w nich swojej kopii. Wielu

właściciele komputerów nieświadomie pozostawia swoje systemy otwarte dla włamywaczy, próbując ułatwić dostęp współpracownikom poprzez udostępnienie folderów do odczytu i zapisu z sieci. Jednakże przy starannej konfiguracji udostępniania zasobów ryzyko ich przejęcia można w znacznym stopniu zmniejszyć.

Anonimowe logowanie

Sesja zerowa (null session), to sesja zestawiona bez podania odpowiednich parametrów uwierzytelnienia (np. z użyciem pustej nazwy użytkownika i pustego hasła). Sesje takie mogą być wykorzystywane do pozyskania informacji o użytkownikach, grupach, udostępnionych zasobach i zasadach dotyczących haseł. Usługi systemu Windows NT, działające na koncie Local System na lokalnym komputerze, komunikują się z innymi usługami przez sieć z użyciem sesji zerowych. Usługi w Windows 2000 i późniejszych, działające na koncie Local System na lokalnym komputerze, używają danych konta lokalnego do uwierzytelnienia się przed innymi usługami. Active Directory w swoim naturalnym trybie nie pozwala na zestawianie sesji zerowych. W trybie mieszanym pozwala na dostęp za pośrednictwem sesji zerowych, dziedzicząc podatności w tym mechanizmie po Windows NT.

Zdalny dostęp do rejestru

Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows 2003, Windows ME oraz Windows XP używają centralnej, hierarchicznej bazy danych, zwanej Rejestrem, do zarządzania oprogramowaniem, konfiguracją urządzeń i ustawieniami użytkownika. Niewłaściwie ustawione prawa dostępu i zasady zabezpieczeń mogą pozwolić na zdalny dostęp do rejestru. Atakujący mogą wykorzystywać tę cechę do przejęcia systemu lub zmiany przypisań plików i praw dostępu tak, by umożliwić wykonanie złośliwego kodu.

Zdalne wywoływanie procedur

Wiele spośród wersji systemów operacyjnych Microsoft (Windows NT 4.0, 2000, XP, oraz 2003) zapewnia mechanizm komunikacji międzyprocesowej, pozwalającej programom działającym na jednej maszynie na zdalne wykonywanie kodu na innej. Zostały opublikowane opisy trzech podatności, pozwalających na wykonanie dowolnego kodu przez atakującego na zaatakowanym systemie z przywilejami Local System. Jedną z tych podatności została wykorzystana przez robaki Blaster/MSblast/LovSAN oraz Nachi/Welchia. Istnieją także inne luki, pozwalające na przeprowadzenie ataku Denial of Service na poszczególne elementy RPC.

W3.2 Podatne systemy operacyjne

Podatne są wszystkie wersje Windows 95, Windows 98, Windows NT Workstation i Server, Windows Me, Windows 2000 Workstation i Server, Windows XP Home i Professional oraz Windows 2003.

W3.3 Wpisy CVE/CAN

NETBIOS

[CVE-2000-0979](#)

[CAN-1999-0518](#), [CAN-1999-0519](#), [CAN-1999-0621](#), [CAN-2000-1079](#)

Anonimowe logowanie

[CVE-2000-1200](#)

Zdalny dostęp do rejestru

[CVE-2000-0377](#), [CVE-2002-0049](#)

[CAN-1999-0562](#), [CAN-2001-0045](#), [CAN-2001-0046](#), [CAN-2001-0047](#), [CAN-2002-0642](#),
[CAN-2002-0649](#), [CAN-2002-1117](#)

Zdalne wywoływanie procedur

[CAN-2002-1561](#), [CAN-2003-0003](#), [CAN-2003-0352](#), [CAN-2003-0528](#), [CAN-2003-0605](#),
[CAN-2003-0715](#)

W3.4 Jak sprawdzić czy Twój system jest podatny na atak?

Jak sprawdzić czy Twój system jest podatny ze względu na problemy z NETBIOS.

Jest wiele narzędzi, które mogą pomóc w stwierdzeniu, czy istnieją w danym systemie podatności związane z NETBIOSem.

NbtScan – NetBIOS Name Network sprawdza obecność usług udostępniania plików NETBIOS na testowanym systemie. NbtScan jest dostępny pod adresem <http://www.inetcat.org/software/nbtscan.html>.

NLTest – potężne narzędzie, zawarte w zestawie Support Tools dla Windows 2000 i 2003 (na dyskach instalacyjnych systemu) oraz w Windows NT4 Resource Kit. Przy pomocy NLTest można zgromadzić wiele informacji o potencjalnych zagrożeniach w konfiguracji.

Użytkownicy Windows 95/98/Me mogą użyć programu Legion v2.11, najnowszej wersji skanera Legion File Share autorstwa Rhino9, aby wyszukać udostępnione zasoby Windows.

Administratorzy Windows 2000 mogą użyć programu Security Fridays Share Password Checker (SPC), aby przeskanować klientów Windows 95/98/Me udostępniające pliki pod kątem ich podatności na możliwość zdalnego uzyskania hasła do udostępnianych zasobów przez atakującego.

Microsoft Baseline Security Advisor może przeskanować systemy Windows NT (SP4), Windows 2000, Windows XP oraz Windows 2003 pod kątem podatności na exploity SMB, a także być użyty do naprawienia problemów. Testy mogą zostać przeprowadzone zarówno zdalnie, jak i lokalnie.

W systemie Windows NT, Windows 2000, Windows XP oraz Windows 2003 użytkownik może wydać z linii poleceń komendę `net share`, aby pozyskać listę udostępnianych zasobów. Więcej informacji o poleceniu net share można uzyskać wpisując net share /?.

WAŻNA Uwaga: Niniejszy artykuł zawiera opis zmian w udostępnianych zasobach. Zanim zmodyfikujesz cokolwiek, upewnij się, że potrafisz przywrócić to do stanu pierwotnego w razie wystąpienia problemów. Zaleca się gruntowne przetestowanie wszelkich zmian przed wdrożeniem ich w środowisku produkcyjnym. Aby dowiedzieć się więcej o udostępnianiu zasobów, zapoznaj się z poniższymi artykułami w Microsoft Knowledge Base:

[125996 - Saving and Restoring Existing Windows Shares](#)

[308419 - HOW TO Set, View, Change, or Remove Special Permissions for Files and](#)

Folders in Windows XP

307874 - HOW TO Disable Simplified Sharing and Password-Protect a Shared Folder in Windows XP

174273 - How to Copy Files and Maintain NTFS and Share Permissions

Domyślne prawa dostępu do udostępnianych zasobów:

Windows NT, Windows 2000, Windows XP (bez Service Packu 1)

- Wszyscy – Pełen dostęp

Windows XP SP1

- Wszyscy - Odczyt

W Windows XP istnieje domyślnie jeden współdzielony folder "SharedDocs." Fizycznie znajduje się on w następującej ścieżce:

"C:\Documents and Settings\All Users\Documents"

- Wszyscy – Pełen dostęp

Większość osiągalnych komercyjnie skanerów sieciowych wykrywa otwarte zasoby udostępnione. Szybki, darmowy i bezpieczny test na obecność udostępniania plików przez SMP i pokrewnych temu podatności w systemie, znaleźć można na [stronie Gibson Research Corporation](#). Należy przejść za odnośnikami do "ShieldsUP", aby otrzymać w czasie rzeczywistym ocenę podatności systemu na atak na SMB. Dostępne są tam także szczegółowe instrukcje postępowania z lukami w SMP dla użytkowników Microsoft Windows. Należy wziąć pod uwagę, że jeśli łączymy się z sieci, w której urządzenie pomiędzy nami i Internetem blokuje ruch SMB, ShieldsUP poinformuje nas, że podatność nie występuje bez względu na to, jak jest w rzeczywistości. Może się bowiem okazać, że kilka tysięcy użytkowników lokalnej sieci kablowej ma możliwość wykorzystania podatności.

Automatyczne skanery wykrywające luki związane z udostępnianiem zasobów:

- [Nessus](#) - darmowy, bardzo mocny, aktualny i łatwy w użyciu zdalny skaner bezpieczeństwa
- [Winfingerprint](#) by vacuum—skaner do enumeracji sieci lub maszyny z Win32

Jak sprawdzić czy Twój system jest podatny na problemy z anonimowym logowaniem.

Spróbuj ustanowić sesję zerową, wydając następującą komendę z linii poleceń systemu:

```
net use \\adres_ip\ipc$ "" /user:""
```

Używając tej składni łączymy się z ukrytym zasobem do połączeń międzyprocesowych IPC\$ pod adresem *adres_ip* jako wbudowany użytkownik anonimowy (/user:"") z pustym hasłem.

Jeżeli otrzymasz komunikat „Wystąpił błąd systemowy 5”, oznacza to, że nastąpiła odmowa dostępu i system nie jest podatny.

Jeśli otrzymasz komunikat o pomyślnym wykonaniu polecenia, oznacza to, że system jest podatny.

Do wykrycia luk związanych z sesją zerową mogą posłużyć także wymienione wyżej Nessus i Winfingerprint.

Jak sprawdzić czy Twój system jest podatny na problemy ze zdalnym dostępem do rejestru.

Pakiet NT Resource Kit (NTRK) autorstwa Microsoftu zawiera plik wykonywalny o nazwie "regdump.exe", który z platformy Windows NT sprawdza w sposób pasywny prawa dostępu do rejestru na innej maszynie z Windows NT/2000 lub XP w sieci lokalnej lub Internecie.

Ponadto, pod poniższym adresem dostępny jest zestaw skryptów dla linii poleceń, które badają prawa dostępu do rejestru oraz całą gamę innych potencjalnych problemów związanych z bezpieczeństwem.

<http://www.afentis.com/top20>.

Jak sprawdzić czy Twój system jest podatny na problemy ze zdalnym wywoływaniem procedur.

Microsoft przygotował narzędzie do sprawdzania konfiguracji i aktualności poprawek - Microsoft Baseline Security Analyzer (MBSA), które zapewnia bodaj najlepszy sposób na zweryfikowanie podatności na wszystkie opisane ataki. MBSA można bezpłatnie pobrać ze strony <http://www.microsoft.com/technet/security/tools/mbsahome.msp>.

Istnieje także samodzielne narzędzie do sprawdzenia, czy w systemie nie brakuje jednej z poprawek CAN-2003-0352, CAN-2003-0528, CAN-2003-0605, CAN-2003-0715 – dostępne pod adresem <http://support.microsoft.com/?kbid=827363>.

Zachęcamy jednak do korzystania z MBSA, ze względu na szersze spektrum jego działania. Użytkownikom w domu czy administratorom mającym pod kontrolą tylko kilka maszyn prawdopodobnie łatwiej będzie skorzystać z witryny

<http://windowsupdate.microsoft.com/> i wyszukać na poszczególnych komputerach brakujące poprawki.

W3.5 Jak się przed tym chronić?

Microsoft reaguje na podatności związane z bezpieczeństwem, wydając dodatki Service Pack oraz poprawki hotfix dla swoich systemów i aplikacji. Dlatego tak ważne jest, by w systemie były zainstalowane aktualne Service Packi oraz poprawki. Na przykład, robak Sasser i jego pochodne (wykorzystujące lukę w LSASS) zainfekowały wiele niezabezpieczonych systemów na całym świecie, podczas gdy systemy z zainstalowaną poprawką MS04-011 były odporne na tę wyjątkowo groźną podatność. Poprawka MS04-011 została wydana przez Microsoft na kilka tygodni przed pojawieniem się Sassera.

UWAGA: Systemy Windows 95 i Windows NT4 Workstation nie są już wspierane przez Microsoft. Wsparcie dla systemu Windows NT4 Server zakończy się 31 grudnia 2004.

Szczegółowe informacje o cyklu życia wspieranych systemów operacyjnych znaleźć można w artykule Microsoft [Product Lifecycle Dates - Windows Product Family](#).

Aby odnaleźć właściwe poprawki dla systemu, można wykorzystać:

- Usługę Windows Update (*Start – Windows Update*). Usługa ta automatycznie wykryje wszystkie wymagane dla danego systemu poprawki i zainstaluje je po uprzedniej akceptacji użytkownika.
- Strona *Security Bulletin Search*:
<http://www.microsoft.com/technet/security/current.aspx>
- Biuletyny bezpieczeństwa Microsoft (po polsku – od lutego 2004):
<http://www.microsoft.com/poland/security/bulletin/default.msp>

Choć zainstalowanie aktualnych dodatków Service Pack i porawek może chronić przed niektórymi błędami w oprogramowaniu (np. błędem przepełnienia bufora), systemy z rodziny Windows posiadają wiele usług, oferujących poprawną i udokumentowaną funkcjonalność, które mogą jednak zostać wyłączone aby podnieść poziom bezpieczeństwa systemu.

Jak chronić się przed atakami związanymi z NETBIOS.

Zmniejszenie ryzyka wykorzystania którejś z podatności udostępnionych zasobów może odbyć się na kilka sposobów:

- Wyłączenie usług Alerter i Posłaniec (Messenger) (są one domyślnie wyłączone w Windows 2003, ale automatycznie włączane w Windows 2000/XP/NT4). Wyłączenie ich w znacznym stopniu zapobiega uzyskiwaniu informacji przez enumerację usług, co ma najczęściej miejsce przed atakiem.
Aby wyłączyć te usługi:
 - wybierz Start – Programy – Narzędzia administracyjne – Usługi
 - wybierz usługę Alerter przez dwukrotne kliknięcie – zmień Typ uruchomienia na Wyłączony – naciśnij Zastosuj - naciśnij Zatrzymaj – naciśnij OK
 - wybierz usługę Posłaniec (Messenger) przez dwukrotne kliknięcie – zmień Typ uruchomienia na Wyłączony – naciśnij Zastosuj – naciśnij Zatrzymaj – naciśnij OK
- Zablokowanie udostępniania zasobów zawsze tam, gdzie nie jest ono niezbędne. Jeżeli dany komputer nie oferuje usług udostępniania plików i drukarek (a tak jest w przypadku większości stacji roboczych w domu i w biurze), można w systemach Windows NT4/2000/2003/XP wyłączyć usługę Serwer. Aby to zrobić:
Wybierz Start – Programy – Narzędzia administracyjne – Usługi – kliknij dwukrotnie usługę Serwer – zmień Typ uruchomienia na Wyłączony – naciśnij Zastosuj – naciśnij Zatrzymaj – naciśnij OK
Jeżeli usługa Serwer musi być uruchomiona, można ją zabezpieczyć w następujący sposób:
 - wylicz wszystkie domyślnie udostępniane zasoby, wydając z linii poleceń systemu komendę

net share
 - usuń zbędne udostępnianie zasobów, wydając z linii poleceń systemu komendę

net share C\$ /delete

Zazwyczaj można bezpiecznie usunąć udostępnianie dysków (C\$, D\$ itd.) oraz zasób ADMIN\$. Nie zaleca się w żadnym systemie usuwania udostępniania zasobu IPC\$

- aby zapewnić zachowanie wprowadzonych zmian (zasoby zostałyby domyślnie uruchomione ponownie przy restarcie systemu lub usługi Serwer), należy zmodyfikować rejestr:
 - uruchom Edytor rejestru (regedit.exe)
 - odnajdź klucz
HKLM\System\CurrentControlSet\Services\lanmanserver\parameters
 - utwórz nowy wpis:
 - nazwa: AutoShareWks
 - typ: DWord
 - wartość: 00000000
 - utwórz nowy wpis:
 - nazwa: AutoShareServer
 - typ: DWord
 - wartość: 00000000
- przejrzyj nie-domyślne (tworzone przez użytkownika) zasoby udostępnione. Można to zrobić, korzystając z:
 - interfejsu graficznego (kliknij prawym klawiszem Mój komputer – Zarządzaj – Foldery udostępnione – Udziały). Wybierz udziały, których udostępnianie chcesz zatrzymać, klikając w nie prawym klawiszem i wybierając Zatrzymaj udostępnianie
 - linii poleceń
 - wylicz wszystkie udostępniane zasoby, wydając polecenie

net share
 - usuń niepotrzebnie udostępniane zasoby poleceniem

net share *NazwaZasobu* /delete

W ten sposób zostanie trwale wyłączone udostępnianie zasobów zdefiniowanych przez użytkownika. Opis trwałego wyłączenia udostępniania zasobów domyślnych znajduje się w poprzednim podpunkcie.

- Klienci z systemem Windows 95/98/Me, wchodzące w skład domeny NT, powinny mieć skonfigurowane prawa dostępu do plików na poziomie użytkownika.
- Nie powinno się pozwalać na dzielenie zasobów z innymi komputerami w Internecie. Wszystkie komputery podłączone bezpośrednio do Internetu powinny mieć usługę udostępniania wyłączoną w panelu kontrolnym Windows. Udostępnianie plików w Internecie powinno się odbywać z użyciem protokołów SCP, FTP i HTTP.
- Nie należy pozwalać na udostępnianie bez uwierzytelnienia. Jeżeli udostępnianie plików jest wymagane, dostęp do folderów powinien być zabroniony, o ile nie dokonano uwierzytelnienia.

- Udostępnianie powinno być ograniczone do minimalnego wymaganego zakresu folderów. Dobrą praktyką jest udostępnianie jednego folderu i ewentualnie folderów w nim zagnieżdżonych.
- Uprawnienia do udostępnianych folderów powinny być ograniczone do minimalnych wymaganych do pracy. W szczególności należy zwrócić uwagę na nadawanie praw do zapisu jedynie w przypadkach, gdy jest to naprawdę niezbędne.
- Dla zwiększenia poziomu bezpieczeństwa, należy wyspecyfikować maszyny, dla których ograniczamy dostęp, przez podanie ich adresów IP, ponieważ nazwy domenowe mogą być znacznie łatwiej sfalszowane.

Jak chronić się przed atakami związanymi z anonimowym logowaniem.

WAŻNA Uwaga: Niniejszy artykuł zawiera informacje o zmianach w rejestrze. Przed wprowadzeniem jakichkolwiek zmian w rejestrze, zrób jego kopię bezpieczeństwa i upewnij się, że potrafisz przywrócić poprzednią zawartość rejestru w razie wystąpienia problemów. Zaleca się gruntowne przetestowanie wszelkich zmian przed wdrożeniem ich w środowisku produkcyjnym. Aby dowiedzieć się, o jak tworzyć kopię rejestru, przywracać ją oraz edytować rejestr, zapoznaj się z poniższymi artykułami w Microsoft Knowledge Base:

[256986 - Description of the Microsoft Windows Registry](#)
[323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0](#)
[322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000](#)
[322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003](#)

Kontrolery domeny Windows NT wymagają sesji zerowych dla potrzeb komunikacji. W związku z tym, korzystając z domeny Windows NT lub z Active Directory w Windows 2000/2003 w trybie mieszanym, pozwalającym na dostęp w standardach starszych niż oferowane przez Windows 2000, można jedynie zmniejszyć ilość informacji, którą można wydobyć przez potencjalny atak. Nie ma natomiast możliwości całkowitego zablokowania dostępu przez ustawienie wartości rejestru RestrictAnonymous na 1. Rozwiązaniem idealnym, możliwym do zastosowania przy korzystaniu wyłącznie z naturalnego trybu działania Active Directory Windows 2000/2003, jest ustawienie wartości RestrictAnonymous na 2.

Aby ograniczyć ilość informacji dostępnych za pośrednictwem sesji zerowych, należy zapoznać się z poniższymi artykułami Microsoft Knowledge Base:

[143474 - Restricting Information Available to Anonymous Logon Users in Windows NT](#)
[246261 - How to Use the RestrictAnonymous Registry Value in Windows 2000](#)

Rozwiązywanie problemów z wartością rejestru RestrictAnonymous opisuje następujący artykuł Microsoft Knowledge Base:

[296405 - The RestrictAnonymous Registry Value May Break the Trust to a Windows 2000 Domain](#)

Jak chronić się przed atakami związanymi ze zdalnym dostępem do rejestru.

Aby zlikwidować zagrożenie, musi zostać ograniczony dostęp do rejestru oraz dokładnie zweryfikowane prawa dostępu do krytycznych jego wartości. W przypadku użytkowników Windows NT 4.0 przed wprowadzaniem zmian konieczna jest instalacja Service Pack 4 (SP4).

WAŻNA Uwaga: Niniejszy artykuł zawiera informacje o zmianach w rejestrze. Przed wprowadzeniem jakichkolwiek zmian w rejestrze, zrób jego kopię bezpieczeństwa i upewnij się, że potrafisz przywrócić poprzednią zawartość rejestru w razie wystąpienia problemów. Zaleca się gruntowne przetestowanie wszelkich zmian przed wdrożeniem ich w środowisku produkcyjnym. Aby dowiedzieć się, jak tworzyć kopię rejestru, przywracać ją oraz edytować rejestr, zapoznaj się z poniższymi artykułami w Microsoft Knowledge Base:

[256986 - Description of the Microsoft Windows Registry](#)

[323170 - HOW TO Backup, Edit, and Restore the Registry in Windows NT 4.0](#)

[322755 - HOW TO Backup, Edit, and Restore the Registry in Windows 2000](#)

[322756 - HOW TO Backup, Edit, and Restore the Registry in Windows XP Windows Server 2003](#)

Ograniczanie dostępu przez sieć. W celu ograniczenia dostępu przez sieć, skorzystaj z poniższej instrukcji, by utworzyć następujący klucz w Rejestrze:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
- Typ: REG_SZ
- Wartość: Registry Server

Prawa dostępu ustawione w tym kluczu określają użytkowników i grupy, które mogą zdalnie dostawać się do rejestru. Przy domyślnej instalacji Windows klucz jest określony i jego zawartość daje pełne uprawnienia użytkownikowi systemowemu Administrator oraz grupie Administratorzy (w Windows 2000 także grupie Operatorzy kopii zapasowych).

Zmiany w rejestrze systemowym wymagają ponownego uruchomienia systemu do zadziałania. Aby utworzyć klucz w rejestrze ograniczający dostęp do rejestru:

1. Uruchom Edytor rejestru (regedt32.exe lub regedit.exe) i przejdź do podklucza: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
2. W menu Edycja, wybierz Nowy klucz
3. Wprowadź następujące wartości:
 - o Nazwa: SecurePipeServers
 - o Typ: REG_SZ
4. Przejdź do podklucza: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
5. W menu Edycja, wybierz Nowy klucz
6. Wprowadź następujące wartości:
 - o Nazwa: winreg
 - o Typ: REG_SZ
7. Przejdź do podklucza: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

8. W menu Edycja, wybierz Nowa wartość ciągu
9. Wprowadź następujące wartości:
 - o Nazwa: Description
 - o Typ: REG_SZ
 - o Wartość: Registry Server
10. Przejdź do podklucza:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
11. Wybierz "winreg." Wybierz Uprawnienia w menu Edycja lub Bezpieczeństwo. Dodaj użytkowników oraz grupy, którym chcesz nadać przywilej dostępu.
12. Zamknij Edytor rejestru i uruchom ponownie Windows.
13. Jeżeli w przyszłości zajdzie potrzeba zmiany listy użytkowników z dostępem do rejestru, powtórz kroki 10-12.

Ograniczenie uprawnionego zdalnego dostępu. Wprowadzenie obostrzeń w dostępie do rejestru ma swoje wady w związku z wykorzystywaniem tego dostępu przez usługi takie jak Directory Replicator czy sieciowa usługa drukowania Spooler.

Możliwe jest wprowadzenie pewnego stopnia szczegółowości w prawach dostępu przez dodanie nazwy konta, z którego korzysta dana usługa, do listy dostępu klucza *winreg* lub przez skonfigurowanie systemu tak, by pomijały ograniczenia dla wyszczególnionych podkluczy przez podanie ich wprost jako wartości Machine i Users w kluczu AllowedPaths:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPaths

Wartość: Machine

Typ: REG_MULTI_SZ – Ciąg wielokrotny

Domyślne dane wartości: System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\Services\EventlogSoftware\Microsoft\WindowsNT\CurrentVersionSystem\CurrentControlSet\Services\Replicator

Zakres: (Poprawna ścieżka w rejestrze)

Opis: Pozwól na dostęp do danej ścieżki w rejestrze, o ile dostęp do niej nie został wprost ograniczony.

Wartość: Users

Typ: REG_MULTI_SZ – Ciąg wielokrotny

Domyślne dane wartości: (brak)

Zakres: (Poprawna ścieżka w rejestrze)

Opis: Pozwól użytkownikom na dostęp do danej ścieżki w rejestrze, o ile dostęp do niej nie został wprost ograniczony.

W rejestrze Microsoft Windows 2000 i Windows XP:

Wartość: Machine

Typ: REG_MULTI_SZ – Ciąg wielokrotny

Domyślne dane wartości: System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\control\Server ApplicationSystem\CurrentControlSet\Services\Eventlog\Software\Microsoft\Windows NT\CurrentVersion

Wartość: Users (domyślnie nie istnieje)

Zazwyczaj jest pewien odstęp czasu między ujawnieniem podatności a udostępnieniem poprawki eliminującej ją. Bywa także, że z powodów związanych z polityką danej firmy, pewne podatności zostają zachowane. Aby zminimalizować zagrożenie, można ograniczać dostęp na brzegach sieci – przez stosowanie firewalli i filtrowanie na routerach. Dodatkowym środkiem może być stworzenie reguł dla systemu IDS, np. [Snort](#), wysyłających alarm lub wywołujących automatyczną akcję.

Jak chronić się przed atakami związanymi ze zdalnym wywoływaniem procedur (RPC).

Zdecydowanie najlepszą metodą jest regularne instalowanie odpowiednich poprawek w miarę ich dostępności przez MBSA lub Windows Update - patrz powyżej: „Jak sprawdzić, czy Twój system jest podatny ze względu na problemy ze zdalnym wywoływaniem procedur”. Gdy jest to niemożliwe, można zdać się na różne sposoby wyłączenia lub ograniczania funkcjonalności RPC. Część z nich opisana jest w znakomitym opracowaniu pod adresem <http://www.ntbugtraq.com/dcomrpc.asp>. UWAGA: wyłączenie czy ograniczanie funkcjonalności RPC może spowodować błędy w działaniu usług Windows, których używasz. W związku z tym, wszelkie zmiany powinny być najpierw testowane poza środowiskiem produkcyjnym.

Jeżeli nie ma możliwości instalowania poprawek, zdecydowanie należy zablokować na brzegach sieci porty używane przez RPC w Windows (porty 135, 139, 445 i 593 TCP; porty 135, 137, 138 i 445 UDP). Oczywiście, zawsze zalecaną praktyką jest domyślne blokowanie na brzegach sieci *wszystkich* nieużywanych usług.

Więcej informacji:

[Artykuł Microsoft Knowledge Base Article 153183. Jak ograniczyć dostęp do rejestru NT ze zdalnego komputera.](#)

[Microsoft Security Bulletin Search.](#)

[MSDN Library](#)

[Microsoft Knowledge Base Article 310426 : HOW TO: Use the Windows XP and Windows Server 2003 Registry Editor](#)

[Network access: Remotely accessible registry paths and subpaths](#)

[Windows Server 2003 Security Guide](#)

[przejdź do początku dokumentu ^](#)

W4 Serwer Microsoft SQL (MSSQL)

W4.1 Opis

Serwer Microsoft SQL (MSSQL) zawiera kilka poważnych luk, pozwalających atakującemu na zdalne zdobycie wrażliwych informacji, zmianę zawartości bazy danych, przejęcie serwerów SQL oraz, w przypadku niektórych konfiguracji, przejęcie systemu, na którym działa serwer.

Podatności MSSQL zostały dobrze opisane i są dość aktywnie atakowane. Dwa ostatnie robaki, ukierunkowane na MSSQL z maja 2002 i stycznia 2003, wykorzystywały kilka znanych luk. Systemy przejęte przez te robaki, wyszukując inne maszyny podatne na infekcję, generowały ruch na poziomie powodującym zakłócenia w pracy sieci.

Dodatkowe informacje o powyższych robakach znaleźć można pod następującymi adresami:

SQLSnake/Spida Worm (maj 2002)

- <http://isc.incidents.org/analysis.html?id=157>
- <http://www.eeye.com/html/Research/Advisories/AL20020522.html>
- http://www.cert.org/incident_notes/IN-2002-04.html

SQL-Slammer/SQL-Hell/Sapphire Worm (styczeń 2003)

- <http://isc.incidents.org/analysis.html?id=180>
- <http://www.nextgenss.com/advisories/mssql-udp.txt>
- <http://www.eeye.com/html/Research/Flash/AL20030125.html>
- <http://www.cert.org/advisories/CA-2003-04.html>

Porty 1433 i 1434 (domyślne porty serwera i monitora MSSQL) są także regularnie wymieniane jako dwa spośród najczęściej skanowanych portów w zestawieniu [Internet Storm Centre](#).

Procedura wykorzystania podatności w SQLSnake opiera się na użyciu domyślnego konta administratora, *sa* – standardowo pozbawionego hasła. Koniecznym warunkiem prawidłowej konfiguracji i ochrony każdego systemu jest zadbanie o to, by wszystkie konta systemowe były chronione hasłem lub wyłączone, jeżeli nie są użytkowane. Więcej informacji o ustalaniu hasła *sa* oraz zarządzaniu nim można znaleźć w artykułach MSDN (Microsoft Developer Network): [Changing the SQL Server Administrator Login](#) oraz [Verify and Change the System Administrator Password by Using MSDE](#). Konto *sa* powinno mieć założone skomplikowane i trudne do odgadnięcia hasło nawet wtedy, gdy nie jest wykorzystywane w danej implementacji SQL/MSDE.

Procedura wykorzystania podatności w SQL Slammerze polegała na przepełnieniu bufora w jednej z usług serwera – Resolution Service. Do przepełnienia bufora i w efekcie przejścia kontroli nad systemem dochodziło na skutek wysłania przez robaka odpowiednio spreparowanego pakietu UDP na port 1434 podatnego serwera. Najskuteczniejszymi sposobami uchronienia się przed takim atakiem jest skrzętna instalacja poprawek, odpowiednia konfiguracja systemu oraz filtrowanie wychodzącego i przychodzącego ruchu (w tym przypadku na port 1434 UDP) na brzegach sieci.

Microsoft Server 2000 Desktop Engine (MSDE 2000) można uważać za „SQL Server Lite”. Wielu użytkowników nie zdaje sobie nawet sprawy, że na ich systemach działa MSDE i że w związku z tym mają zainstalowany także serwer SQL. MSDE 2000 jest instalowane jako część następujących pakietów Microsoft:

- SQL/MSDE Server 2000 (Developer, Standard and Enterprise Editions)
- Visual Studio .NET (Architect, Developer and Professional Editions)
- ASP.NET Web Matrix Tool
- Office XP
- Access 2002
- Visual Fox Pro 7.0/8.0

Istnieje wiele innych pakietów, które używają oprogramowania MSDE 2000. Aktualną listę znaleźć można pod adresem:

<http://www.SQLsecurity.com/forum/applicationslistgridall.aspx>. Ponieważ oprogramowanie to używa MSDE jako mechanizmu obsługi bazy danych, zawiera ono te same luki, co serwer SQL/MSDE. Sposób nasłuchiwanie MSDE 2000 na połączenia klienckie można skonfigurować na wiele sposobów. Można umożliwić łączenie się przez named pipe po sesji NetBIOS (porty 139/445 TCP) lub standardowo na port TCP 1433 albo stosować oba sposoby jednocześnie. Niezależnie od wybranej metody, serwer SQL i MSDE zawsze będzie nasłuchiwał na porcie 1434 UDP. Ten port został wybrany jako port monitora, do którego kierowane jest pierwsze zapytanie od klienta. Z odpowiedzi na nie klient dowiaduje się, w jaki sposób ma ustanowić połączenie z serwerem.

Serwer MSDE 2000 wysyła informacje na swój temat w odpowiedzi na jednobajtowy pakiet 0x02 na port 1434 UDP. Inne jednobajtowe pakiety mogą powodować przepełnienie bufora, bez konieczności jakiegokolwiek uwierzytelnienia się przez klienta.

Sprawę pogarsza fakt, że cały atak odbywa się przez protokół UDP. Niezależnie od tego czy proces MSDE działa na poziomie zaufania użytkownika domeny, czy lokalnego konta SYSTEM, pomyślnie wykorzystanie przytoczonych podatności może oznaczać całkowite przejście kontroli nad zaatakowanym systemem.

Ponieważ SQL Slammer wykorzystuje przepełnienie bufora na zaatakowanym systemie, receptą jest stosowanie się do dobrych praktyk instalowania poprawek w odpowiednim czasie oraz starannej konfiguracji systemu. W sprawdzeniu podatności danego systemu na ten atak, a także wyszukaniu w całej domenie czy sieci podatnych systemów i zainstalowaniu na nich odpowiednich krytycznych poprawek pomoże [Zestaw aktualizacji krytycznej do programu SQL](#).

Warto zapoznać się z raportem i analizami na stronach incidents.org, aby poznać więcej szczegółów dotyczących robaka SQL Slammer. Jego atak dotknął w poważny sposób szkieletu sieci Internet rankiem 25 stycznia 2003 r.

W4.2 Podatne systemy operacyjne

Każdy system Microsoft Windows z zainstalowanym Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 lub Microsoft SQL/MSDE Server Desktop Engine 2000, oraz każdy system, na którym używane jest MSDE.

W4.3 Wpisy CVE/CAN

[CVE-1999-0999](#), [CVE-2000-0202](#), [CVE-2000-0402](#), [CVE-2000-0485](#), [CVE-2000-0603](#), [CVE-2001-0344](#), [CVE-2001-0879](#)

[CAN-2000-0199](#), [CAN-2000-1081](#), [CAN-2000-1082](#), [CAN-2000-1083](#), [CAN-2000-1084](#), [CAN-2000-1085](#), [CAN-2000-1086](#), [CAN-2000-1087](#), [CAN-2000-1088](#), [CAN-2000-1209](#), [CAN-2001-0509](#), [CAN-2001-0542](#), [CAN-2002-0056](#), [CAN-2002-0154](#), [CAN-2002-0186](#), [CAN-2002-0187](#), [CAN-2002-0224](#), [CAN-2002-0624](#), [CAN-2002-0641](#), [CAN-2002-0642](#), [CAN-2002-0643](#), [CAN-2002-0644](#), [CAN-2002-0645](#), [CAN-2002-0649](#), [CAN-2002-0650](#), [CAN-2002-0695](#), [CAN-2002-0721](#), [CAN-2002-0729](#), [CAN-2002-0859](#), [CAN-2002-0982](#), [CAN-2002-1123](#), [CAN-2002-1137](#), [CAN-2002-1138](#), [CAN-2002-1145](#), [CAN-2003-0118](#)

W4.4 Jak sprawdzić czy Twój system jest podatny na atak?

Microsoft opublikował zestaw narzędzi poświęconych bezpieczeństwu SQL

<http://www.microsoft.com/sql/downloads/securitytools.asp>. Tzw. Zestaw aktualizacji krytycznej dla programu SQL zawiera cenne narzędzia, takie jak: SQL Scan, SQL

Check, i Krytyczna aktualizacja SQL.

Chip Andrews z sqlsecurity.com opracował narzędzie SQLPingv2.2. Wysyła ono jednobajtowy pakiet UDP o zawartości 0x02 na port 1434 – pojedynczego hosta lub całej podsięci. Serwer SQL nasłuchujący na porcie 1434 UDP odpowie informacjami na swój temat – numerem wersji, ilością instancji, itp. SQLPingv2.2 uważany jest za skaner podobny do SQL Scan autorstwa Microsoft i nie powoduje przejścia systemu ani naruszenia bezpieczeństwa skanowanej sieci. To i inne narzędzia dla bezpieczeństwa SQL znaleźć można na stronie Chipa Andrewsa: SQL/MSDE Security Web site.

W4.5 Jak się przed tym chronić?

W skrócie:

1. Wyłącz SQL/MSDE Monitor Service na porcie UDP 1434.
2. Zainstaluj aktualny service pack dla serwera Microsoft SQL/MSDE i/lub MSDE 2000.
3. Zainstaluj aktualną poprawkę zbiorczą, opublikowaną później niż ostatni service pack.
4. Zainstaluj wszystkie indywidualne poprawki opublikowane później niż ostatnia poprawka zbiorcza.
5. Włącz logowanie zdarzeń uwierzytelnienia do serwera SQL.
6. Zabezpiecz serwer na poziomie systemu oraz sieci.
7. Zminimalizuj uprawnienia, z którymi uruchomione są serwer i agenci MSSQL/MSDE.

Szczegółowo:

1. Wyłącz SQL/MSDE Monitor Service na porcie UDP 1434.

Łatwo to zrealizować poprzez instalację a następnie posłużenie się funkcjonalnością [SQL Server 2000 Service Pack 3a](#). Engine bazy danych MSDE 2000 zawiera dwie podatności na przepełnienie bufora, dające się wykorzystać zdalnie i bez uwierzytelnienia. Sprawę pogarsza fakt, że cały atak odbywa się przez protokół UDP. Niezależnie od tego czy proces MSDE działa na poziomie zaufania użytkownika domeny, czy lokalnego konta SYSTEM, pomyślnie wykorzystanie przytoczonych podatności może oznaczać całkowite przejście kontroli nad zaatakowanym systemem. MS-SQL Slammer wysyła pakiety o długości 376 bajtów na port 1434 UDP pod losowo wybrane adresy z bardzo dużą częstotliwością. Przejęte systemy same zaczynają wysyłać takie same pakiety od momentu infekcji. Robak wybiera adresy losowo, włączając w to adresy typu multicast, powodując w sieci Denial of Service. W przypadku pojedynczych zainfekowanych maszyn notowano ruch na poziomie 50 Mb/s.

2. Zainstaluj aktualny service pack dla serwera Microsoft SQL/MSDE i/lub MSDE 2000.

Aktualne (w momencie powstawania tego dokumentu) wersje service pack dla serwerów MSSQL/MSDE to:

- o SQL/MSDE Server 7.0 Service Pack 4
- o MSDE/SQL Server 2000 Service Pack 3a

Aby być pewnym, że aktualność service pack jest zachowana, należy sprawdzać regularnie serwis [Make Your SQL/MSDE Servers Less Vulnerable](#), będący częścią Microsoft TechNet.

3. Zainstaluj aktualną poprawkę zbiorczą, opublikowaną później, niż ostatni service pack.

Aktualną (w momencie powstawania tego dokumentu) poprawką zbiorczą dla wszystkich wersji serwera SQL/MSDE jest [MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks \(Q316333/Q327068\)](#).

Aby być pewnym, że poprawki zbiorcze są aktualne, należy szukać bieżących poprawek zbiorczych dla serwera SQL/MSDE pod następującymi adresami:

- o [Microsoft SQL/MSDE Server 7.0](#)
- o [Microsoft SQL Server 2000](#)
- o [MSDE Server Desktop Engine 2000 \(MSDE 2000\)](#)

4. Zainstaluj wszystkie indywidualne poprawki opublikowane później, niż ostatnia poprawka zbiorcza.

W momencie powstawania tego dokumentu nie było żadnej poprawki indywidualnej opublikowanej później, niż [MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks \(Q316333/Q327068\)](#).

Aby być pewnym, że poprawki indywidualne są aktualne, należy szukać bieżących poprawek dla serwera SQL/MSDE pod następującymi adresami:

- o [Microsoft SQL/MSDE Server 7.0](#)
- o [Microsoft SQL Server 2000](#)
- o [MSDE Server Desktop Engine 2000 \(MSDE 2000\)](#)

5. Włącz logowanie zdarzeń uwierzytelnienia do serwera SQL.

Logowanie zdarzeń uwierzytelnienia (SQL Server Authentication Logging) jest zazwyczaj wyłączone. Można je włączyć, korzystając z aplikacji Enterprise Manager (Server properties; zakładka Security).

6. Zabezpiecz serwer na poziomie systemu oraz sieci.

Jedną z najczęściej atakowanych podatności w MSSQL/MSDE jest fakt, że domyślne konto administratora, *sa*, instalowane jest z pustym hasłem. Pozostawiając je bez ochrony hasłowej, w istocie pozostawia się serwer całkowicie niezabezpieczony i podatny na ataki robaków oraz innych exploitów. W związku z tym, należy zastosować się do zaleceń rozdziału „System Administrator (SA) Login” w dokumencie [SQL/MSDE Server Books Online](#) i upewnić się, że wbudowane konto *sa* ma silne hasło nawet wtedy, gdy nie jest ono używane w danej instalacji SQL/MSDE. W bazie MSDN znajdują się dokumenty [Changing the SQL Server Administrator Login](#) oraz [Verify and Change the System Administrator Password by Using MSDE](#), których lektura także może okazać się przydatna.

7. Zminimalizuj uprawnienia, z którymi uruchomione są serwer i agenci MSSQL/MSDE.

Uruchom serwer MSSQL/MSDE oraz agenta SQL/MSDE na koncie użytkownika domeny z minimalnymi uprawnieniami, a nie na koncie administratora domeny, SYSTEM (w NT), czy LocalSystem (w 2000 lub XP). Przejęta usługa, działająca z uprawnieniami lokalnymi lub w domenie, daje atakującemu całkowitą kontrolę nad maszyną i/lub siecią.

- Włącz uwierzytelnienie w Windows NT, kontrolę udanych i nieudanych logowań Enable Windows NT Authentication, enable auditing for successful and failed logins, po czym zatrzymaj i uruchom na nowo usługę MSSQL/MSDE. W miarę możliwości, skonfiguruj klientów tak, by korzystali z uwierzytelnienia do NT.
- Filtrowanie pakietów powinno odbywać się na brzegach sieci, aby blokować nieuprawnione przychodzące i wychodzące połączenia z usługami MSSQL. Filtrowanie przychodzących i wychodzących pakietów na porty 1433 oraz 1434 TCP i UDP powinno uniemożliwić atakującym wewnątrz i na zewnątrz sieci lokalnej skanowanie i infekcję podatnych serwerów MSSQL i MSDE.
- Jeżeli porty 1433 i 1434 muszą być dostępne z Internetu, skonfiguruj dostęp do nich tak, by możliwe było filtrowanie ruchu przychodzącego i wychodzącego, uniemożliwiające nadużycia z wykorzystaniem tych portów.

Więcej informacji o zabezpieczaniu serwera Microsoft SQL/MSDE znaleźć można pod poniższymi adresami:

- [Microsoft SQL/MSDE Server 7.0 Security](#)
- [Microsoft SQL/MSDE Server 2000 Security](#)

[przejdź do początku dokumentu ^](#)

W5 Uwierzytelnienie w Windows

W5.1 Opis

Hasła i kody bezpieczeństwa wykorzystywane są niemal w każdym przypadku interakcji pomiędzy użytkownikiem i systemem informatycznym. Większość form uwierzytelnienia użytkownika, podobnie jak ochrony danych i plików, opiera się na hasle podawanym przez użytkownika. Ponieważ prawidłowo przeprowadzone uwierzytelnienie często nie jest odnotowywane (a nawet jeśli zostaje odnotowane, zazwyczaj nie wzbudza podejrzeń), przejęte hasło użytkownika to doskonała okazja do rozpoznania systemu od wewnątrz w sposób niemal niezauważalny. Atakujący, posługując się takim hasłem, zapewnia sobie dostęp do wszelkich zasobów udostępnionych użytkownikowi oraz znajduje się znacznie bliżej możliwości penetracji innych kont w systemie, maszyn w sąsiedztwie czy przejęcia uprawnień administratora. Pomijając powyższe zagrożenie, konta ze słabymi lub pustymi hasłami pozostają wciąż na porządku dziennym, a organizacje z wdrożoną dobrą polityką dotyczącą haseł pozostają rzadkością.

Najczęściej występujące słabości związane z użyciem haseł to:

- Konta użytkowników bez hasła lub z hasłem zbyt słabym.
- Słaba ochrona hasła przez użytkownika – niezależnie od siły samego hasła.
- Konta administracyjne tworzone przez system lub aplikacje, które pozbawione są haseł lub mają hasła zbyt słabe.

- Funkcje skrótu dla haseł są znane, a same skróty przechowywane bywają w sposób umożliwiający powszechny do nich dostęp. Najlepszą ochroną jest w tym przypadku wdrożenie polityki, zawierającej szczegółowe wskazówki dla użytkowników jak tworzyć hasła i postępować z nimi oraz rutynowe, prewencyjne sprawdzanie integralności haseł.

Microsoft Windows nie przechowuje ani nie przesyła haseł otwartym tekstem – do uwierzytelnienia używa ich skrótów. Skróty jest to wynik działania funkcji matematycznej, zwanej funkcją skrótu, na arbitralnie wybranej ilości danych. W Windows istnieją trzy mechanizmy uwierzytelnienia: LM (najmniej bezpieczny, najbardziej kompatybilny), NTLM i NTLMv2 (najbezpieczniejszy, najmniej kompatybilny). Choć większość obecnie działających implementacji Windows nie wymaga wsparcia dla LAN Manager (LM), w Windows NT, 2000 i XP (ale nie w Windows 2003) domyślnie trzymane są lokalnie skróty haseł LM (tzw. LANMAN hashes). Ponieważ LM używa znacznie słabszego algorytmu szyfrującego, niż bardziej współczesne NTLM i NTLMv2, hasła LM mogą zostać bardzo łatwo i szybko złamane. Nawet takie hasła, które należałoby uznać za mocne w normalnych okolicznościach, mogą być złamane metodą brute-force w ciągu mniej niż tygodnia z użyciem dostępnych dziś mocy obliczeniowych.

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/h_gly.asp

Słabość skrótów LM wynika z następujących cech:

- Hasła ucinane są do pierwszych 14 znaków.
- Hasła są uzupełniane spacjami do długości 14 znaków.
- Litery w hasle zamieniane są na wielkie.
- Hasła są przechowywane w siedmioznakowych łańcuchach znaków.

Taki proces oznacza, że zadanie włamywacza zostaje zredukowane do odgadnięcia dwóch siedmioznakowych haseł, składających się z wielkich liter. Ponieważ złożoność problemu złamania skrótu wzrasta geometrycznie wraz z długością skrótu, każdy łańcuch siedmioznakowy jest przynajmniej o rząd wielkości łatwiejszy do złamania metodą brute-force niż połączony łańcuch czternastoznakowy. Ponieważ każdy łańcuch jest dokładnie siedmioznakowy (włączając spacje) i nie zawiera małych liter, atak słownikowy jest także znacznie łatwiejszy do przeprowadzenia. W związku z tym metoda wyliczania skrótu w algorytmie LM stoi w całkowitej opozycji do jakiegokolwiek dobrej polityki zarządzania hasłami.

Poza ryzykiem posiadania zapisanych skrótów haseł w postaci LM, uwierzytelnienie poprzez LM jest też często domyślnie włączone na maszynach klienckich i akceptowane przez serwer. W rezultacie, maszyny z możliwością używania silniejszych algorytmów, mogą posługiwać się znacznie słabszym LM do przesyłania skrótów haseł w sieci. Oczywiście, takie skróty mogą zostać przechwycone przez podsłuch pakietów i następnie łatwo złamane.

W5.2 Podatne systemy operacyjne

Wszystkie wersje systemów Microsoft Windows.

W5.3 Wpisy CVE/CAN

[CVE-2000-0222](#)

[CAN-1999-0504](#), [CAN-1999-0505](#), [CAN-1999-0506](#)

W5.4 Jak sprawdzić czy Twój system jest podatny na atak?

Choć jest wiele obserwowalnych oznak ogólnej słabości haseł – takich jak istnienie w systemie kont użytkowników, którzy rozstali się z daną organizacją lub serwisów, które nie są używane – jedynym sposobem przekonania się, że hasła wszystkich użytkowników są dostatecznie mocne, jest zastosowanie tych samych narzędzi, których do łamania haseł używają komputerowi włamywacze.

Uwaga: Nigdy nie uruchamiaj narzędzia do łamania haseł, nawet na systemach, na których masz uprawnienia administratora, bez wyraźnej, najlepiej pisemnej zgody kierownictwa/pracodawcy. Zdarzało się, że administratorów, którzy mieli jak najlepsze intencje, zwalniano za działanie bez pozwolenia.

Do najlepszych dostępnych programów łamiących hasła należą: [LC4 \(l0phtcrack version 4\)](#) i [John the Ripper](#).

Jeżeli chodzi o lokalnie przechowywane skróty LAN Manager:

- Jeżeli używasz systemu NT, 2000 lub XP zainstalowanego w sposób domyślny, to Twój system jest niestety podatny, ponieważ skróty LM są w tych systemach domyślnie przechowywane.
- Jeżeli masz w swoim środowisku produkcyjnym zaszciości w postaci systemów wymagających uwierzytelnienia LM do komunikacji z serwerem, to systemy te oraz całe środowisko są podatne, ponieważ maszyny te wysyłają skróty LM, które mogą zostać przechwycone z ruchu sieciowego.

W5.5 Jak się przed tym chronić?

Najlepszą i najbardziej stosowną ochroną przed słabymi hasłami jest silna polityka zarządzania hasłami, która zawiera szczegółowe instrukcje w zakresie nauczania użytkownika dobrych zwyczajów zarządzania hasłami, a także uwzględnia sprawdzanie integralności haseł przez administratorów, udzielając im pełnego poparcia kierownictwa organizacji. Aby stworzyć dobrą politykę w tym zakresie, należy podjąć następujące kroki:

- **Zadbaj o silne hasła.** Posiadając wystarczającą ilość sprzętu i czasu, każde hasło może być złamane za pomocą ataku brutalnego. Oprogramowanie łamiące hasła (*password crackers*), często wykorzystywane przez atakujących, wykonują atak słownikowy. Ponieważ najpowszechniejsze algorytmy szyfrowania haseł są znane, narzędzia te po prostu porównują skrót wszystkich słów w słowniku (w wielu językach), a także imion, oraz ich różnych permutacji, ze skrótem hasła. Tak więc, każde hasło które przypomina jakiś wyraz w dowolnym języku, jest podatne na atak słownikowy. Wiele organizacji zachęca użytkowników do tworzenia haseł z uwzględnieniem znaków alfanumerycznych i specjalnych. W konsekwencji użytkownicy biorą jakiś wyraz (np.: *password*) i zmieniają litery na cyfry bądź znaki specjalne (np.: *pa\$\$w0rd*). Takie permutacje nie chronią przeciwko atakowi słownikowemu: prawdopodobieństwo złamania *pa\$\$w0rd* jest podobne do prawdopodobieństwa złamania *password*.

Dobre hasło nie może pochodzić od wyrazu lub imienia. Silna polityka zarządzania hasłami powinna nakazywać użytkownikom generowanie hasła z

czegoś bardziej losowego, jak na przykład fraza, dłuższy tytuł książki bądź piosenki. Poprzez złączenie dłuższej frazy w hasło (na przykład, branie pierwszej litery każdego wyrazu we frazie, ustanawiając wielkie i małe litery, lub podmiana znaku specjalnego zamiast słowa, i/lub zamiana wszystkich samogłosek na znaki specjalne w tak stworzonym hasle), użytkownicy mogą wygenerować odpowiednio długie hasła, z odpowiednimi kombinacjami znaków alfanumerycznych i znaków specjalnych, w sposób utrudniający ich złamanie metodą ataku słownikowego. A jeżeli pierwotną frazę było łatwo zapamiętać, to samo powinno dotyczyć hasła.

Kiedy użytkownicy otrzymają odpowiednie instrukcje jak tworzyć dobre hasła, szczegółowe procedury powinny być wyznaczone, w celu upewnienia się, czy instrukcje te są przestrzegane. Najlepszym sposobem zapewnienia takiej kontroli jest weryfikacja siły hasła przy każdej jego zmianie przez użytkownika przy pomocy programu Passfilt (NT4).

Windows 2000, XP oraz 2003 mają bardzo mocne narzędzia do wymuszania stosowania silnych haseł. Aby przejrzeć aktualne zasady dotyczące haseł stosowane w systemie, należy otworzyć: (Start - Ustawienia – Panel sterowania – Narzędzia administracyjne – Zasady zabezpieczeń lokalnych – Zasady konta – Zasady haseł). Zasady haseł mają następujące ustawienia:

- **Hasła muszą spełniać wymagania co do złożoności.** Określa, czy hasła muszą spełniać wymagania złożoności. Wymagania te są narzucane przy tworzeniu i zmianie hasła. Jeżeli opcja jest włączona, hasło musi spełniać następujące wymagania minimalne:
 - Nie może zawierać w całości lub w części nazwy konta użytkownika
 - Musi mieć co najmniej 6 znaków
 - Musi zawierać znaki z trzech spośród czterech następujących grup:
 - Wielkie litery alfabetu angielskiego (A do Z)
 - Małe litery alfabetu angielskiego (a do z)
 - 10 cyfr (od 0 do 9)
 - Znaki specjalne (np.: , !, \$, #, %)
- **Wymuszaj tworzenie historii haseł (zakres: 0-24):** Określa liczbę unikalnych haseł, które muszą być wykorzystane dla konta danego użytkownika, zanim system pozwoli na ponowne użycie starego hasła. Wartość może zostać ustalona z przedziału 0-24. Ustalenie wartości parametru na 0 pamiętanych haseł umożliwia ciągłe używanie tego samego hasła. Ustalenie jej na 24 oznacza wymuszenie użycia 24 różnych haseł, zanim ponownie zostanie użyte pierwsze z nich. Ta opcja pozwala na podniesienie poziomu bezpieczeństwa przez zapewnienie, że stare hasła nie są wciąż na nowo używane. Aby zachować skuteczność działania tej opcji należy wykluczyć możliwość natychmiastowej zmiany hasła przez skonfigurowanie minimalnego okresu ważności hasła.
- **Maksymalny okres ważności hasła (zakres: 0-999 dni):** Określa czas (w dniach), przez jaki może być używane hasło, zanim system wymusi na użytkownika jego zmianę. Można ustalić wygasanie hasła po pewnej liczbie dni (pomiędzy 1 a 999) lub wyłączyć wygasanie hasła przez ustawienie wartości na 0.

- **Minimalny okres ważności hasła (zakres: 0-999 dni):** Określa czas (w dniach), przez jaki musi być używane hasło, zanim użytkownik będzie mógł je zmienić. Można ustalić wartość pomiędzy 1 i 999 dni lub pozwolić na natychmiastową zmianę hasła przez ustalenie wartości na 0. Minimalny okres ważności hasła musi być mniejszy niż maksymalny okres ważności hasła. Ustal minimalny okres ważności hasła na wartość większą niż 0, jeżeli chcesz, żeby wymuszanie tworzenia historii haseł było skuteczne. Bez narzucenia minimalnego okresu ważności hasła, użytkownik może zmieniać je raz po razie tak długo, aż system pozwoli mu na nowo nadać jego stare, ulubione. Ustawienie domyślne nie spełnia tego zalecenia, aby administrator mógł ustalić hasło użytkownikowi, po czym wymóc na nim jego zmianę. Jeżeli wymuszanie tworzenia historii haseł ustawione jest na 0, użytkownik nie musi wymyślać nowego hasła. Z tego powodu, wymuszanie tworzenia historii ma domyślnie wpisaną wartość 1.
- **Minimalna długość hasła (zakres: 0-14 znaków):** Określa najmniejszą ilość znaków jaką może zawierać hasło dla konta użytkownika. Można wybrać wartość z zakresu od 1 do 14 znaków lub ustalić, że hasło nie jest w ogóle wymagane, wpisując wartość 0. Minimalna długość hasła powinna być zgodna z długością określoną w polityce bezpieczeństwa firmy – w innym przypadku zaleca się ustalenie minimalnej długości hasła na 8 lub więcej znaków ([National Security Agency \(NSA\)](#) zaleca minimum 12 znaków).
- **Zapisz hasła wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego:** Określa, czy system Windows 2000, 2003 lub XP Professional będzie przechowywał hasła korzystając z szyfrowania odwracalnego. Opcja ta zapewnia wsparcie dla aplikacji, których protokół uwierzytelnienia wymaga znajomości hasła użytkownika. W zasadzie przechowywanie haseł zapisanych z użyciem szyfrowania odwracalnego jest równoważne przetrzymywaniu ich w formie otwartego tekstu. W związku z tym, z opcji tej nie należy korzystać, chyba że konieczność używania danej aplikacji jest wyższa niż konieczność ochrony haseł.

Istnieje możliwość automatycznego wygenerowania skomplikowanych haseł i przydzielenia ich użytkownikom przez wywołanie polecenia (z linii poleceń Windows NT4, 2000, XP, 2003):

```
net user username /random
```

Wykonanie tego polecenia przydzieli losowe skomplikowane (lecz zawsze ośmioznakowe) hasło do konta *username* i wyświetli je na konsoli. Sposób ten wydaje się jednak bardziej odpowiedni dla haseł przydzielanych usługom niż rzeczywistym użytkownikom.

Najlepszym sposobem na sprawdzenie jakości haseł jest wykorzystanie programu do ich łamania jako fragment procedury rutynowego wewnętrznego skanowania.

Ważna uwaga: Nigdy nie uruchamiaj narzędzia do łamania haseł, nawet na systemach, na których masz uprawnienia administratora, bez wyraźnej, najlepiej pisemnej zgody kierownictwa/pracodawcy. Zdarzało się, że administratorów, którzy mieli jak najlepsze intencje, zwalniano za działanie bez pozwolenia.

Kiedy już masz pozwolenie na łamanie haseł na Twoim systemie, rób to regularnie na odpowiednio zabezpieczonym, również fizycznie, systemie. Użytkownicy, którym złamano hasło, powinni zostać powiadomieni dyskretnie, a następnie poinstruowani, jak lepiej dobierać hasła. Procedury powiadamiania użytkowników w takich przypadkach powinny być opracowane wspólnie przez administratorów i kierownictwo organizacji, jako część polityki zarządzania hasłami tak, aby kierownictwo zapewniło wsparcie w sytuacji, w której użytkownicy nie reagują na uwagi administratorów.

Inna możliwość w zakresie ochrony przed pustymi lub słabymi hasłami to zastosowanie alternatywnej formy uwierzytelnienia, np. tokenu generującego hasła czy biometrii.

1. **Chroń silne hasła.** Nawet jeśli hasła same w sobie są dość silne, konta do których są przypisane mogą zostać przejęte, jeżeli hasła te nie będą należycie chronione przez użytkowników. W dobrze skonstruowanej polityce powinny zostać uwzględnione zakazy udostępniania hasła innym osobom, zapisywania ich w sposób umożliwiający niepowołany dostęp do nich i nakaz należytego zabezpieczenia plików zawierających hasła służące do automatycznego uwierzytelnienia (w istocie dużo łatwiej jest chronić hasła, gdy stosowanie takich metod uwierzytelnienia ograniczy się do przypadków absolutnej konieczności). Należy także wymusić wygasanie haseł, co sprawia, że słabe hasła, które z jakichś przyczyn nie zostały wyeliminowane przez inne polityki, są używane jedynie przez krótki okres czasu. Starych haseł nie powinno się używać ponownie. Dobrą praktyką jest uprzedzanie użytkowników o kończącym się wkrótce okresie ważności ich hasła. Gdy na ekranie pojawia się komunikat „Twoje hasło wygasło i musi zostać zmienione”, użytkownicy będą bardziej skłonni wybrać słabe hasło.
2. **Dokładnie kontroluj konta.**
 - Każde konto administratora lub usługi, które nie jest wykorzystywane, powinno być wyłączone, a jeżeli możliwe, usunięte. Każde konto administratora bądź usługi, które jest wykorzystywane, powinno mieć ustanowione nowe i silne hasło, od razu po instalacji usługi/konta.
 - Regularnie wykonuj audyt kont na systemach i sporządź listę wszystkich tych kont lub usług wymagających istnienia tego konta i poziomu wymagań na konto. Pamiętaj też o kontach i hasłach na systemach takich jak routery, switchy, cyfrowe drukarki podpięte do sieci, kopiarki i serwery drukarek.
 - Opracuj dokładne procedury dodawania/usuwania upoważnionych kont do/z listy.
 - Regularnie sprawdzaj listę, w celu upewnienia się czy nie dodano nowych kont i że niewykorzystywane konta zostały usunięte.
 - Stwórz procedury usuwania kont, kiedy pracownicy bądź użytkownicy kontraktowi odchodzą z pracy lub kiedy konta te nie są dalej potrzebne.
3. **Utrzymuj politykę zarządzania hasłami w firmie.** Oprócz kontroli na poziomie systemu operacyjnego czy usług sieciowych, istnieje wiele rozbudowanych narzędzi, które mogą pomóc we wdrażaniu polityki zarządzania

hasłami. Wiele przykładowych szablonów takiej polityki, wskazówek odnośnie wdrożeń, opisów podstaw bezpieczeństwa haseł oraz odnośników do stron z politykami zarządzania hasłami znaleźć można na stronie [SANS Security Policy Project](#).

4. **Wyłącz uwierzytelnienie LM poprzez sieć.** Najlepszym substytutem dla LAN Managera w Windows jest NT LAN Manager version 2 (NTLMv2). Zastosowany w nim protokół wyzwanie-odpowiedź znosi wiele ze słabości LM przez użycie silniejszego szyfrowania oraz poprawione mechanizmy uwierzytelnienia i zabezpieczenia sesji. Klucz w rejestrze, pozwalający na kontrolę tej funkcjonalności zarówno w Windows NT jak i 2000 to:

Gałąź: HKEY_LOCAL_MACHINE
Klucz: System\CurrentControlSet\Control\LSA
Wartość: LMCompatibilityLevel
Typ wartości: REG_DWORD - Number
Zakres wartości: 0-5
Wartość domyślna: 0

Opis: Parametr ten określa rodzaj wykorzystywanego uwierzytelnienia.

- 0 – Wysyłaj odpowiedzi LM i NTLM; nigdy nie używaj zabezpieczeń sesji NTLMv2
- 1 – Użyj zabezpieczeń sesji NTLMv2, jeżeli uda się je wynegocjować
- 2 – Wysyłaj wyłącznie uwierzytelnienie NTLM
- 3 – Wysyłaj wyłącznie uwierzytelnienie NTLMv2
- 4 – Kontroler Domeny odmawia użycia uwierzytelnienia LM
- 5 – Kontroler Domeny odmawia użycia uwierzytelnienia LM i NTLM (zezwala jedynie na NTLMv2)

W Windows 2000, 2003 i XP tę samą funkcjonalność można osiągnąć, konfigurując ustawienia Poziom uwierzytelnienia LAN Manager (Windows 2000) lub Zabezpieczenia sieci: Poziom uwierzytelnienia LAN Manager (Windows XP, 2003) (Start – Ustawienia – Panel sterowania – Narzędzia administracyjne – Zasady zabezpieczeń lokalnych – Zasady lokalne – Opcje zabezpieczeń).

Jeżeli wszystkie systemy w danym środowisku to Windows NT z Service Pack 4 lub nowsze, aby zapobiec jakiegokolwiek transmisji skrótów LM poprzez sieć, można ustawić wartość opcji na 3 na wszystkich stacjach klienckich oraz 5 na wszystkich kontrolerach domeny. Starsze systemy (np. Windows 95/98) nie potrafią jednakże korzystać z NTLMv2 przy pomocy standardowego oprogramowania Microsoft Network Client. Aby móc używać funkcjonalności NTLMv2, należy zainstalować Directory Services Client. Po instalacji dostępna jest wartość rejestru „LMCompatibility” z możliwymi parametrami 0 lub 3.

W razie braku możliwości narzucenia korzystania z NTLMv2 na starszych klientach, można dokonać drobnej poprawy w stosunku do LM przez wymuszenie NTLM (NT LAN Manager version 1) po stronie kontrolera domeny (ustawiając LMCompatibilityLevel na 4 lub wybierając odpowiednie ustawienie w karcie Opcje zabezpieczeń). Najbezpieczniejszym rozwiązaniem problemu zasłochi w systemach operacyjnych jest jednak ich wymiana na nowe wersje,

ponieważ stare nie zapewniają wsparcia dla minimalnego choćby poziomu bezpieczeństwa.

5. **Zapobiegaj przechowywaniu skrótów LM.** Problemem, który pozostaje po wyeliminowaniu przesyłania skrótów LM przez sieć jest fakt, że skróty te są nadal tworzone i zapisywane w SAM lub Active Directory. Microsoft zapewnił mechanizm pozwalający na całkowite wyłączenie tworzenia skrótów LM, ale jest on dostępny wyłącznie w Windows 2000, 2003 oraz XP. W systemie Windows 2000 z Service Pack 2 lub późniejszym odpowiedzialny jest za to następujący wpis w rejestrze:

Gałąź: HKEY_LOCAL_MACHINE

Klucz: System\CurrentControlSet\Control\LSA\NoLMHash

Jeżeli na kontrolerze domeny Windows 2000 zostanie utworzony powyższy klucz, skróty LanMan nie będą tworzone i przechowywane w ActiveDirectory.

W Windows XP i 2003 tę samą funkcjonalność można uzyskać włączając opcję Zabezpieczenia sieci: Nie przechowuj wartości mieszania (hash) programu LAN Manager dla następnej zmiany hasła (Start – Ustawienia – Panel sterowania – Narzędzia administracyjne – Zasady zabezpieczeń lokalnych – Zasady lokalne – Opcje zabezpieczeń).

Po wprowadzeniu powyższych zmian, aby mogły one zadziałać, system musi zostać ponownie uruchomiony.

Ważna uwaga: Zmiany powyższe zapobiegają jedynie tworzeniu nowych skrótów LM. Te już istniejące będą pojedynczo usuwane w miarę, jak poszczególni użytkownicy będą zmieniać swoje hasła.

6. **Zabezpiecz skróty haseł i bazę SAM przed skopiowaniem.** Narzędzia do łamania haseł, o których wspomnieliśmy w tym rozdziale wymagają uprzedniego zdobycia skrótów. Może to zostać zrealizowane przez:

- Podłuch haseł z sieci. Przeciwdziałanie: 1. Użycie sieci z przełącznikami (switch); 2. Wykrywanie i usuwanie kart sieciowych działających w trybie promiscuous (potrafi je wykrywać większość komercyjnego oprogramowania do kontroli poziomu bezpieczeństwa oraz wiele narzędzi darmowych, np. [ethereal](#)).
- Kopiowanie pliku SAM (znajduje się on w folderze %SystemRoot%\System32\Config\; zazwyczaj jest to C:\Winnt\System32\Config\ w Windows NT4 i 2000 lub C:\Windows\System32\Config\ w Windows XP i 2003). Plik ten jest w czasie normalnej pracy zablokowany przez system operacyjny i może zostać skopiowany jedynie, gdy komputer zostanie uruchomiony z innym systemem. SAM może także zostać pozyskany z kopii bezpieczeństwa. Jest on też zapisywany na Dysku awaryjnym NT4.

Przeciwdziałanie: Ograniczenie i nadzór dostępu fizycznego do systemów komputerowych (w szczególności kontrolera domeny), nośników kopii zapasowych i dysków awaryjnych.

Następujące artykuły ze stron Microsoft zawierają pożyteczne informacje dodatkowe:

- [How to Disable LM Authentication on Windows NT \[Q147706\]](#) - opisuje szczegółowe zmiany, które należy wprowadzić w rejestrze Windows 9x i Windows NT/2000, aby wyłączyć uwierzytelnienie LM.
- MS03-034 : Flaw in NetBIOS Could Lead to Information Disclosure (824105)
- [LMCompatibilityLevel and Its Effects \[Q175641\]](#) wyjaśnia problemy dotyczące współpracy systemów, związanych z ustawieniem LMCompatibilityLevel.
- [How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT \[Q239869\]](#) – opisuje sposób wykorzystania Directory Services Client z Windows 2000, aby obejść problem zgodności z NTLMv2 w Windows 95/98.
- [New Registry Key to Remove LM Hashes from Active Directory and Security Account Manager](#) – opisuje, jak usunąć skróty LM z Active Directory i SAM.

[przejdź do początku dokumentu ^](#)

W6 Przeglądarki WWW

W6.1 Opis

Dzięki przeglądarkom użytkownicy systemów Microsoft Windows uzyskują dostęp do sieci. Dominującą pozycję wśród przeglądarek ma Internet Explorer (IE), domyślnie instalowany w systemie Microsoft Windows. Wśród innych przeglądarek należy wymienić Mozillę, Firefox, Netscape oraz Operę. Najnowszą wersją IE, którą opisywać będziemy tutaj, jest wersja 6. Opisywane podatności dotyczą także Mozilli w wersjach 1.-1.7.1, Firefox w wersji 0.9.x, Netscape w wersji 7.x oraz Opery w wersji 7.x.

Problemy z IE można podzielić na sześć rodzajów:

1. Znaczna liczba luk w ciągu ostatnich kilku lat w porównaniu z innymi przeglądarkami – 153 podatności w IE od kwietnia 2001, według [Security Focus Archive](#).
2. Długi czas potrzebny na załatanie znanych luk w IE – Użytkownikom kazano czekać nawet ponad sześć miesięcy od opublikowania informacji o luce, do wydania łaty przez Microsoft.
3. Active X i Active Scripting w IE – Luki w IE, w szczególności wykorzystujące ActiveX, pozwalały na obejście innych zabezpieczeń wbudowanych w system i przejęcie maszyny.
4. Znaczna liczba niezalotanych luk - 34, według <http://umbrella.name/originalvuln/msie/>
5. Podatność na Spyware/Adware – Problem ten dotyczy wszystkich przeglądarek, ale IE jest podatna bardziej niż inne przeglądarki.
6. Integracja przeglądarki IE z jądrem systemu operacyjnego, sprawiająca, że system staje się bardziej podatny na atak.

Oczywiście, problemy występują także w pozostałych przeglądarkach, jednak w żadnej z nich nie są one tak poważne jak w przypadku IE. Złośliwy autor serwisu WWW może utworzyć stronę w taki sposób, że luki w przeglądarce zostaną wykorzystane przy zwykłym przeglądaniu serwisu. Doskonałym przykładem takiego działania był problem "[Download.Ject](#)". Luka, którą wykorzystano istniała od wielu miesięcy i związana była ze słabościami ActiveX. Mimo opublikowania wykorzystującego ją kodu [8 czerwca 2004](#), pozostała niezalotana aż do lipca 2004. Ze względu na połączenie ActiveX, języków skryptowych i swoją integrację z system operacyjnym Windows, Internet Explorer jest bardziej podatny na ataki niż jakakolwiek inna przeglądarka.

Konsekwencjami udanego ataku mogą być: ujawnienie danych z cookies, z lokalnych plików, wykonanie lokalnych programów, pobranie i wykonanie dowolnego kodu czy wreszcie całkowite przejęcie systemu.

W6.2 Podatne systemy operacyjne

Opisywane luki dotyczą systemów Microsoft Windows, korzystających z jednej z wymienionych przeglądarek. Co ważne, przeglądarka IE jest instalowana wraz z wieloma produktami Microsoft i dlatego występuje niemal we wszystkich systemach Windows, nawet jeżeli użytkownik nigdy nie zamierzał jej instalować i używać. Wszystkie inne przeglądarki instalowane są na życzenie użytkownika i od niego zależy wykorzystanie ich przez inne aplikacje.

W6.3 Podatności przeglądarek, według Secunia

A. Internet Explorer:

2004 - 15 Zaleceń dot. bezpieczeństwa Secunia (stan na 30 lipca 2004)

1. [Microsoft Internet Explorer Multiple Vulnerabilities](#)
2. [Internet Explorer Frame Injection Vulnerability](#)
3. [Internet Explorer File Download Error Message Denial of Service Weakness](#)
4. [Internet Explorer Security Zone Bypass and Address Bar Spoofing Vulnerability](#)
5. [Internet Explorer Local Resource Access and Cross-Zone Scripting Vulnerabilities](#)
6. [Microsoft Internet Explorer and Outlook URL Obfuscation Issue](#)
7. [Windows Explorer / Internet Explorer Long Share Name Buffer Overflow](#)
8. [Microsoft Outlook Express MHTML URL Processing Vulnerability](#)
9. [Internet Explorer/Outlook Express Restricted Zone Status Bar Spoofing](#)
10. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
11. [Internet Explorer Cross Frame Scripting Restriction Bypass](#)
12. [Internet Explorer File Identification Variant](#)
13. [Internet Explorer Travel Log Arbitrary Script Execution Vulnerability](#)
14. [Internet Explorer File Download Extension Spoofing](#)
15. [Internet Explorer showHelp\(\) Restriction Bypass Vulnerability](#)

B. Luki w Mozilli

2004 - 7 Zaleceń dot. bezpieczeństwa Secunia

1. [Mozilla Fails to Restrict Access to "shell:"](#)
2. [Mozilla XPInstall Dialog Box Security Issue](#)
3. [Multiple Browsers Frame Injection Vulnerability](#)
4. [Mozilla Browser Address Bar Spoofing Weakness](#)
5. [Mozilla / NSS S/MIME Implementation Vulnerability](#)
6. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
7. [Mozilla Cross-Site Scripting Vulnerability](#)

D. Luki w Nestcape

2004 - 2 Zalecenia dot. bezpieczeństwa Secunia

1. [Mozilla Fails to Restrict Access to "shell:"](#)
2. [Multiple Browsers Frame Injection Vulnerability](#)

E. Luki w Operze

2004 - 8 Zaleceń dot. bezpieczeństwa Secunia

1. [Opera Browser Address Bar Spoofing Vulnerability](#)
2. [Multiple Browsers Frame Injection Vulnerability](#)
3. [Opera Address Bar Spoofing Security Issue](#)

4. [Opera Browser Favicon Displaying Address Bar Spoofing Vulnerability](#)
5. [Multiple Browsers Telnet URI Handler File Manipulation Vulnerability](#)
6. [Opera Browser Address Bar Spoofing Vulnerability](#)
7. [Multiple Browser Cookie Path Directory Traversal Vulnerability](#)
8. [Opera Browser File Download Extension Spoofing](#)

W6.4 Identyfikacja i ochrona przed podatnościami w przeglądarkach

Jeżeli w swoim systemie korzystasz z Internet Explorera, nie istnieje sposób, by stwierdzić, czy Twój system jest podatny, ponieważ istnieje zbyt wiele niezalotanych luk w tej przeglądarce. Mimo to, należy regularnie odwiedzać serwis [Windows Update](#) aby upewnić się, że system chroniony jest przynajmniej przed tymi lukami, na które zostały wydane łatki. Użytkownicy zainteresowani dalszą ochroną przed podatnościami w przeglądarkach powinni rozważyć jedną z poniższych opcji:

- a. Należy rozważyć korzystanie z innej przeglądarki, nie wykorzystującej ActiveX. Większość serwisów WWW nie wykorzystuje ActiveX. Ponieważ takie podejście skutecznie uniemożliwi korzystanie ze strony Windows Update, wykorzystującej ActiveX, należy użyć mechanizmu [Automatycznego Uaktualniania](#). Alternatywą mogą być narzędzia takie jak [Shavlik's HFNetChkPro™](#) czy [Microsoft Baseline Security Analyzer \(MBSA\)](#). Ponadto, narzędzia do analizy bezpieczeństwa IE online, np. [Qualys Browser Check](#), mogą być nieocenione w ustaleniu poziomu zabezpieczenia przeglądarki IE.
- b. Jeżeli opcja a. okaże się trudna do zastosowania, np. ze względu na wykorzystanie ActiveX w sieci intranetowej, należy rozważyć wykorzystywanie IE do przeglądania zasobów intra- a innej przeglądarki do internetowych.
- c. Jeżeli wykorzystanie innej przeglądarki w ogóle nie jest możliwe, należy rozważyć całkowite wyłączenie ActiveX za wyjątkiem użycia wewnętrznych apletów ActiveX, które mogą zostać wcześniej zainstalowane na danej maszynie. Microsoft umożliwia skonfigurowanie Internet Explorera w sposób uniemożliwiający wykonywanie kontrolek ActiveX.

W przypadku innych przeglądarek nie dysponujemy automatycznymi narzędziami podobnymi do tych dla Internet Explorera. Używając Mozilli/Firefox, Netscape'a lub Opery, należy regularnie odwiedzać strony ich producentów (<http://www.mozilla.org>, <http://www.netscape.com>, <http://www.opera.com>), lub stronę <http://umbrella.name/index.html> by czerpać stamtąd informacje o wykrytych lukach i dostępnych poprawkach.

W6.5 Jak zabezpieczyć Internet Explorer

Aby skonfigurować zabezpieczenia w Internet Explorerze:

1. Wybierz Opcje internetowe z menu Narzędzia.
2. Wybierz zakładkę Zabezpieczenia i kliknij Poziom niestandardowy dla strefy zawartości Internet.

Większość luk w IE wykorzystywana jest poprzez aktywne skrypty lub kontrolki ActiveX.

3. W Obsługa skryptów, zaznacz Wyłącz przy Pozwól na operacje wklejania przez skrypt, aby zapobiec niepowołanemu odczytowi danych ze schowka.

Uwaga: Wyłączenie Active Scripting może spowodować, że niektóre witryny WWW przestaną działać.

Kontrolki ActiveX są mniej popularne, lecz potencjalnie groźniejsze, bowiem zezwalają na większy dostęp do systemu.

4. Zaznacz Wyłącz przy Pobieranie podpisanych formantów ActiveX.
5. Zaznacz Wyłącz przy Pobieranie niepodpisanych formantów ActiveX.
6. Zaznacz Wyłącz przy Inicjowanie i wykonywanie skryptów formantów ActiveX nie zaznaczonych jako bezpieczne.

Aplety języka Java mają zazwyczaj większe możliwości niż skrypty.

7. Pod Microsoft VM, zaznacz Wysokie bezpieczeństwo przy Uprawnienia Java, aby prawidłowo odizolować środowisko apletu Javy i chronić system przed niepowołanym dostępem.
8. Pod Różne zaznacz Wyłącz przy Dostęp do źródła danych poprzez domeny, aby uchronić się przed atakami cross-site scripting.

Należy także upewnić się, że żadne niezauwane adresy nie znajdują się w strefie Zaufane witryny bądź Lokalny intranet, ponieważ strefy te mają z założenia słabsze poziomy zabezpieczeń.

[przejdź do początku dokumentu ^](#)

W7 Aplikacje wymiany plików

W7.1 Opis

Programy peer to peer są wykorzystywane przez rosnącą rzeszę użytkowników. Służą do pobierania i dystrybucji rozmaitych rodzajów danych (np. muzyki, filmów, obrazów, tekstu, kodu źródłowego itp.). Aplikacje P2P mają wiele legalnych zastosowań, takich jak wymiana oprogramowania OpenSource/GPL, obrazów ISO bootowalnych dystrybucji Linuxa, dzieł niezależnych twórców a nawet mediów komercyjnych, np. wersji preview gier i zwiastunów filmów. Często jednak dane wymieniane w sieciach P2P są wątpliwego pochodzenia lub są chronione prawami autorskimi. Po problemach prawnych, które dotknęły Napstera, większość obecnie używanych aplikacji P2P działa w oparciu o rozproszoną sieć klientów, udostępniających foldery lub całe dyski z danymi. Użytkownik może wprowadzić kryteria wyszukiwania za pośrednictwem aplikacji klienckiej, po czym pomiędzy użytkownikami zestawiane jest jedno lub więcej połączeń transmisyjnych, za pośrednictwem których oprogramowanie wyszukuje żądany plik. Klienci działają zarówno jako aplikacje pobierające dane, serwer udostępniający dane, oraz w przypadku niektórych sieci, jako superwęzły koordynujące wymianę danych między użytkownikami.

Komunikacja Peer to Peer składa się z zapytań, odpowiedzi i transferów plików. Uczestnik sieci może jednocześnie pobierać wiele plików oraz w tym samym czasie pozwalać na pobieranie wielu plików. Wyszukiwanie danej zawartości może być przeprowadzane według dowolnych łańcuchów znaków. Większość aplikacji P2P używa w chwili obecnej portów domyślnych, umożliwiając jednak ich automatyczną bądź ręczną zmianę w celu uniknięcia wykrycia, zablokowanie przez firewalle lub inne filtry ruchu. Wydaje się, że aktualnym trendem jest przechodzenie do wykorzystania wrapperów http, aby łatwiej omijać restrykcje wprowadzane przez firmowe polityki bezpieczeństwa. Wielowątkowość wyszukiwania i transferu plików może powodować znaczące zwiększenie ruchu, zwłaszcza w gęstych sieciach lokalnych, prowadząc do

całkowitego wykorzystania pasma na połączeniu z siecią rozległą.

W związku z oprogramowaniem P2P mamy do czynienia z podatnościami, które można zaliczyć do trzech kategorii. Podatności natury technicznej mogą być wykorzystywane zdalnie. Podatności natury socjotechnicznej mogą być wykorzystane przez podmianę plików binarnych poszukiwanych przez użytkowników. Z podatnościami natury prawnej mamy do czynienia w związku z naruszeniami praw autorskich i wykorzystaniem materiałów o kontrowersyjnej zawartości.

Jak wspomniano wyżej, podatności techniczne mogą być wykorzystywane zdalnie i pochodzić z prostego działania pobrania, instalacji i wykonania danych aplikacji. Wpisy CVE i CAN wymienione poniżej dotyczą właśnie podatności technicznych. Ich skutki mogą obejmować zakres od zablokowania systemu (DoS) po dostęp do dowolnych plików. Powinno się je traktować bardzo poważnie. Co prawda nie opisane w CVE i CAN, lecz nie mniej poważne są sprawy związane z ochroną prywatności i poufności przy korzystaniu z aplikacji P2P. Wiele z tych programów zawiera składniki typu *spyware* czy *adware*, zużywające pasmo na informowanie swoich autorów o stronach odwiedzanych przez użytkownika aplikacji. Źle skonfigurowana aplikacja P2P potrafi umożliwić nieautoryzowany dostęp do całej sieci przez udostępnienie zmapowanych dysków sieciowych. Nie ma praktycznie żadnych ograniczeń w odniesieniu do rodzaju danych, jakie mogą zostać udostępnione w sieci P2P, czego skutkiem może być przejście informacji poufnych, własności intelektualnych i innych.

Z podatnością socjotechniczną mamy do czynienia, gdy złośliwy lub wcześniej zainfekowany użytkownik tworzy lub zmienia plik tak, by przypominał treści poszukiwane przez innych. Plik taki może zawierać wirusa, konia trojańskiego czy inne złośliwe oprogramowanie. Ofiarą takiego ataku staje się zwykle użytkownik o mniejszej wiedzy technicznej, który otworzy plik nie orientując się, że ikona czy rozszerzenie pliku nie odpowiadają standardowo przypisanemu spodziewanemu typowi danych lub daje się nakłonić do otwarcia pliku wykonywalnego. Niezależnie od rodzaju danych wymienianych przez P2P, użytkownik takiego oprogramowania powinien korzystać z programów antywirusowych do skanowania pobieranych plików. Tam, gdzie to możliwe, należy także sprawdzać sumy kontrolne plików aby upewnić się, że to co zostało pobrane jest w istocie tym, co mieliśmy zamiar pobrać, a autor udostępnić. Ruch P2P może także służyć do tunelowania ruchu sterującego przejętymi maszynami (zombie).

Podatności natury prawnej powinny być poważnie brane pod uwagę zarówno przez użytkowników korporacyjnych jak i domowych. Treści dostępne w sieciach P2P zawierają także materiały chronione prawami autorskimi, m.in. muzykę, filmy i oprogramowanie. Organizacje takie jak [MPAA](#), [RIAA](#) i [BSA](#) aktywnie starają się zwalczyć łamanie praw autorskich w sieciach P2P. Wezwania sądowe, pozwy i nakazy trafiają do sądów w całym Stanach Zjednoczonych. Ich sukcesy lub niepowodzenia a także (nie)moralność użytkowników pobierających wymienione materiały to sprawy drugorzędne w porównaniu z kosztami ponoszonymi przez firmy w związku z oskarżeniami. W sieciach P2P jest także powszechnie dostępna pornografia. Kwestia jej legalności jest również drugorzędna w porównaniu z kwestią ewentualnego pozwu o molestowanie seksualne, który mógłby złożyć przeciw firmie jej pracownik, znalazłszy na służbowym komputerze materiały ściągnięte z sieci P2P przez innego pracownika.

W7.2 Podatne systemy operacyjne

Istnieją wersje aplikacji P2P dla wszystkich systemów operacyjnych Windowsa także dla systemów UNIX i Linux.

W7.3 Wpisy CVE/CAN

[CAN-2000-0412](#), [CVE-2001-0368](#), [CAN-2002-0314](#), [CAN-2002-0315](#), [CVE-2002-0967](#), [CAN-2003-0397](#)

W7.4 Jak stwierdzić czy Twój system jest podatny na atak?

Wykrycie ruchu P2P w sieci może być wyzwaniem. Można wyszukiwać ruch P2P przez monitorowanie ruchu na portach najczęściej używanych przez te aplikacje lub wyszukiwanie w ruchu wzorców charakterystycznych dla danych aplikacji. Na końcu tej sekcji znajduje się lista portów najczęściej używanych przez aplikacje P2P. Istnieją także programy pomagające w wykrywaniu i blokowaniu ruchu P2P. Niektóre systemy zapobiegania intruzom (ISP) typu host-based mogą zapobiegać instalacji i uruchamianiu aplikacji P2P. Cisco Network Based Application Recognition (NBAR) i inne produkty sieciowe mogą zablokować ruch P2P wchodzący i wychodzący z sieci lub pozwalać na monitorowanie tego ruchu. Monitorowanie połączeń w sieci WAN z użyciem aplikacji takich jak NTOP może także pomóc w wykryciu ruchu P2P. Można także wyszukiwać na serwerach plików typy plików najczęściej pobierane z sieci P2P - .mp3, .wma, .avi, .mpg, .mpeg, .jpg, .gif, .zip, .torrent czy .exe. Przydaje się też sprawdzanie folderów sieciowych pod kątem szybko kurczącej się przestrzeni dyskowej. Istnieje wtyczka do Nessusa, wykrywająca działające oprogramowanie P2P, a w przypadku maszyn z systemem Windows, można do przeskanowania programów zainstalowanych na poszczególnych maszynach wykorzystać SMS.

W7.5 Jak się przed tym chronić?

Polityki firmowe:

1. Firma powinna posiadać i egzekwować politykę zabraniającą pobierania materiałów chronionych prawem autorskim.
2. Firma powinna posiadać i egzekwować politykę korzystania z firmowego łącza internetowego.
3. Powinno być przeprowadzane regularne przeglądanie serwerów plików i stacji roboczych pod kątem zabronionych materiałów.

Ograniczenia sieciowe:

1. Zwykłym użytkownikowi należy zabronić instalowania oprogramowania na swoich stacjach – w szczególności aplikacji P2P.
2. Należy rozważyć wykorzystanie serwera proxy, kontrolującego dostęp do Internetu.
3. Filtrowanie ruchu wychodzącego powinno wykluczać korzystanie z portów, które nie są wykorzystywane do potrzeb służbowych. Jednakże migracja ruchu P2P w stronę portów wykorzystywanych przez typowe usługi, np. http, obniża skuteczność tego podejścia.
4. Należy szukać ruchu P2P w sieci i we właściwy sposób odnosić się do przypadków naruszenia polityk firmowych.
5. Należy wykorzystać oprogramowanie antywirusowe w skali firmy, w szczególności upewniając się, że dokonywane są aktualizacje wzorców wirusów.

Porty najczęściej wykorzystywane przez aplikacje P2P

Napster

eDonkey

Gnutella

Kazaa

tcp 8888	tcp 4661	tcp/udp 6345	tcp 80 (WWW)
tcp 8875	tcp 4662	tcp/udp 6346	tcp/udp 1214
tcp 6699	udp 4665	tcp/udp 6347	
		tcp/udp 6348	

Wpisy w bazie sygnatur programu Snort: <http://www.snort.org/cgi-bin/signs-search.cgi?sid=p2p>

- 549 [P2P napster login](#)
- 550 [P2P napster new user login](#)
- 551 [P2P napster download attempt](#)
- 552 [P2P napster upload request](#)
- 556 [P2P Outbound GNUTella client request](#)
- 557 [P2P GNUTella client request](#)
- 559 [P2P Inbound GNUTella client request](#)
- 561 [P2P Napster Client Data](#)
- 562 [P2P Napster Client Data](#)
- 563 [P2P Napster Client Data](#)
- 564 [P2P Napster Client Data](#)
- 565 [P2P Napster Server Login](#)
- 1383 [P2P Fastrack \(kazaa/morpheus\) GET request](#)
- 1432 [P2P GNUTella GET](#)
- 1699 [P2P Fastrack \(kazaa/morpheus\) traffic](#)
- 2180 [P2P BitTorrent announce request](#)
- 2181 [P2P BitTorrent transfer](#)

[przejdź do początku dokumentu ^](#)

W8 LSASS

W8.1 Opis

Usługa Windows Local Security Authority Subsystem Service w Windows 2000, Server 2003 i Server 2003 64 Bit oraz XP i XP 64 Bit zawiera krytyczny błąd przepełnienia bufora, którego wykorzystanie może prowadzić do przejęcia pełnej kontroli nad systemem. Atak może zostać przeprowadzony zdalnie i anonimowo przez RPC w systemach Windows 2000 i XP. Wymaga natomiast przyznanych lokalnie przywilejów w Windows 2003 Server i Windows XP 64 Bit.

LSASS odgrywa kluczową rolę w systemie uwierzytelnienia i funkcjonalności Active Directory. Tutaj, w części odpowiadającej za współpracę z Active Directory, w jednej z funkcji logujących LSASRV.dll może zostać przepełniony bufor przez przesłanie zbyt długiego łańcucha. Potencjalnie, może to doprowadzić do przejęcia systemu.

Ciężar faktu, że luka daje się łatwo wykorzystać zdalnie, został wykazany przez ostatnią propagację robaków Sasser i Korgo, opartych na kodzie wykorzystującym

LSASS. Robaki te znane są też jako W32.Sasser (<http://www.cert.org/current/archive/2004/07/12/archive.html#sasser>, <http://www.microsoft.com/security/incident/sasser.msp>) i W32.Korgo (<http://www.cert.org/current/archive/2004/07/12/archive.html#korgo>). Wiele spośród złośliwych "botów" także wykorzystuje lukę w LSASS a jej waga wśród problemów bezpieczeństwa stale rośnie, choć często nie jest to dostrzegane.

Luka w LSASS otrzymała w CVE oznaczenie CAN-2003-0533. Administratorom zaleca się nie tylko załatanie systemów, ale także zastosowanie wszelkich niezbędnych mechanizmów kontroli dostępu na stykach sieci aby zapobiec rozprzestrzenianiu się zagrożeń związanych z mechanizmami RPC na podatne środowiska.

W8.2 Podatne systemy operacyjne

Windows 2000, Windows XP Home Edition i Professional, Windows XP 64 Bit Edition, Windows 2003

W8.3 Wpisy CVE/CAN

[CVE-1999-0227](#)

[CAN-1999-1234](#), [CAN-2001-1122](#), [CAN-2003-0507](#), [CAN-2003-0533](#),
[CAN-2003-0663](#), [CAN-2003-0818](#)

W8.4 Jak sprawdzić czy Twój system jest podatny na atak?

Lukę można wykryć zarówno zdalnie, jak i lokalnie w systemie. Wykrywanie zdalne jest metodą zalecaną administratorom sieci, których zadaniem jest zapewnienie bezpieczeństwa w pewnym zakresie adresów IP. Kontrola z poziomu systemu jest dobrym rozwiązaniem dla pojedynczych użytkowników, którzy chcą sprawdzić, czy ich system jest bezpieczny.

Do detekcji zdalnej można posłużyć się jednym z następujących, darmowych narzędzi:

1. Nessus – sieciowy skaner bezpieczeństwa – zawiera wtyczkę smb_kb835732, sprawdzającą, czy łąta KB835732 jest zainstalowana w systemie. Szczegóły i pliki do pobrania: <http://cgi.nessus.org/plugins/dump.php3?id=12209>.
2. DSScan autorstwa Foundstone pozwala na przeskanowanie całej sieci i wysłanie ostrzeżeń do zagrożonych systemów. Szczegóły i pliki do pobrania: <http://www.foundstone.com/resources/proddesc/dsscan.htm>.
3. Sasser Worm Scanner autorstwa eEye sprawdza, czy system jest podatny na wykorzystanie luki w LSASS oraz robaka Sasser. Szczegóły i pliki do pobrania: <http://www.eeye.com/html/resources/downloads/audits/index.html>.

Do detekcji lokalnej nadają się narzędzia Microsoft:

1. Microsoft Baseline Security Analyzer (MBSA) pozwala na stwierdzenie czy system jest podatny na wykorzystanie luki w LSASS. Szczegóły i pliki do pobrania: <http://www.microsoft.com/technet/security/tools/mbsahome.msp>.
2. Windows Update przegląda system i udostępnia wybór poprawek dobrany pod kątem konkretnej maszyny. Jeżeli wśród dostępnych poprawek jest także MS04-011 (KB835732), oznacza to, że nie jest ona jeszcze zainstalowana, a więc system jest podatny. Instrukcje krok po kroku na stronie <http://windowsupdate.microsoft.com>.

W8.5 Jak się przed tym chronić?

W skrócie:

1. Zablokuj porty na firewallu
2. Zainstaluj aktualną poprawkę z Microsoft
3. Włącz zaawansowane filtrowanie ruchu TCP/IP

W szczegółach:

1. Zablokuj porty na firewallu

Jeżeli masz do dyspozycji firewall, ochronę sieci przed atakami z zewnątrz zapewni zablokowanie następujących portów:

- UDP/135, UDP/137, UDP/138, UDP/445
- TCP/135, TCP/139, TCP/445, TCP/593

Zaleca się skorzystanie z firewalla osobistego instalowanego na maszynie i zablokowanie wszelkiego niepożądanego ruchu przychodzącego. Jeżeli używasz Zapory połączenia internetowego (ICF) wbudowanej w Windows XP i Windows Server 2003, ruch przychodzący blokowany jest domyślnie. Zaporę połączenia internetowego można włączyć następująco:

- a. kliknij Start – Panel sterowania
- b. wybierz Połączenia sieciowe i telefoniczne
- c. kliknij prawym klawiszem połączenie, z którego korzystasz i wybierz Właściwości
- d. otwórz zakładkę Zaawansowane
- e. zaznacz Chroń mój komputer.... i kliknij OK

Uwaga! Jeżeli potrzebujesz umożliwić komunikację niektórych programów i usług przez firewall, otwórz zakładkę Zaawansowane i wybierz Ustawienia, a następnie zdefiniuj programy, protokoły i usługi, z których chcesz korzystać.

2. Zainstaluj aktualną poprawkę w zależności od używanej wersji systemu Windows

Poprawka na lukę w LSASS jest dostępna pod adresem:

<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>

3. Włącz zaawansowane filtrowanie TCP/IP aby zablokować ruch przychodzący
 - a. kliknij Start – Panel sterowania – Połączenia sieciowe i telefoniczne
 - b. kliknij prawym klawiszem połączenie, które chcesz skonfigurować i wybierz Właściwości
 - c. pod Właściwości połączenia w zakładce Ogólne wybierz Protokół TCP/IP i kliknij Właściwości
 - d. w oknie dialogowym Właściwości protokołu TCP/IP wybierz Zaawansowane
 - e. wybierz zakładkę Opcje
 - f. wybierz Filtrowanie TCP/IP – Właściwości
 - g. zaznacz opcję Włącz filtrowanie TCP/IP (wszystkie karty)
 - h. do dyspozycji masz trzy kolumny
 - Porty TCP
 - Porty UDP
 - Protokoły IP

W każdej z kolumn należy wybrać jedną z opcji:

- Pozwalaj wszystkim. Zaznacz tę opcję, jeśli chcesz pozwolić na przepuszczanie wszystkich pakietów TCP lub UDP
- Pozwalaj tylko. Zaznacz tę opcję, jeśli chcesz pozwolić na przepuszczanie jedynie określonego ruchu TCP lub UDP. Kliknij Dodaj i wpisz odpowiedni port lub numer protokołu w oknie dialogowym. Nie możesz zablokować ruchu TCP lub UDP, wybierając Pozwalaj tylko w kolumnie Protokoły IP, a następnie wpisując wartości 6 i 17.

Uwaga! Konfigurując filtrowanie TCP/IP pamiętaj, które porty musisz zablokować. W szczególności, aby zabezpieczyć się przed wykrozystaniem luki w LSASS, musisz zablokować port TCP/445 w ruchu przychodzącym.

[przejdź do początku dokumentu ^](#)

W9 Klient poczty elektronicznej

W9.1 Opis

Microsoft Outlook to menadżer informacji osobistych połączony z klientem pocztowym dla Microsoft Windows. Używany przede wszystkim jako aplikacja do obsługi poczty elektronicznej, zapewnia jednak funkcjonalność znacznie szerszą, oferując m.in. kalendarz, zarządzanie zadaniami i kontaktami. W połączeniu z serwerem Microsoft Exchange, Microsoft Outlook oferuje także wsparcie dla wielu użytkowników, pomoc w koordynacji terminów spotkań, wspólne kalendarze i skrzynki pocztowe.

Outlook Express (OE), darmowa wersja Outlooka o mocno ograniczonej funkcjonalności, zapewniającej w podstawowym stopniu zarządzanie elektroniczną korespondencją i bazą kontaktów. OE jest rozprowadzany w pakiecie wraz z przeglądarką Internet Explorer od wersji 1.0. Ta z kolei jest integralną częścią wszystkich systemów Microsoft Windows, począwszy od wersji 95. Ostatnia wersja Outlook Expressa, 6.0 z SP1, jest dostępna do darmowego pobrania. Dzięki włączaniu produktów takich jak Internet Explorer i Outlook Express w inne linie produktów, w tym Office, BackOffice i sam system Windows, wspólne technologie i fragmenty kodu mogą być używane pomiędzy platformami. Niestety, takie rozwiązanie wprowadza krytyczne, najłabsze ogniwa łańcucha oraz sprawia, że potencjalna luka ma znacznie poważniejszy wydźwięk.

Jednym z celów Microsoft był rozwój łatwego w użyciu i intuicyjnego narzędzia do obsługi poczty elektronicznej i informacji. Niestety, zaszyte mechanizmy automatyzacji doprowadziły do powstania podatności, które wykorzystali twórcy wirusów, robaków i złośliwych programów przejmujących lokalny system oraz autorzy innych form ataków.

Do potencjalnych zagrożeń związanych z korzystaniem z klienta poczty elektronicznej należy zaliczyć:

- Zarażenie komputera wirusem lub robakiem – złośliwym kodem, rozprzestrzeniającym się przez załączniki lub skrypty zaszyte w treści wiadomości;
- Spam – niepożądaną korespondencję;
- Weryfikacja adresów email wyzwalana otwarciem wiadomości przez odbiorcę.

Aktualne wersje Outlooka i OE pozwalają na ochronę przed powyższymi zagrożeniami, pod warunkiem ich poprawnego skonfigurowania.

W9.2 Podatne systemy opracyjne

Wszystkie wersje systemu Microsoft Windows zawierają Outlook Express w pakiecie z Internet Explorerem. Dlatego też wszystkie wersje należy uznać za potencjalnie

podatne.

Aktualnie zainstalowaną wersję OE rozpoznać można uruchamiając Internet Explorera i wybierając opcję Internet Explorer – Informacje z menu Pomoc. Wersje starsze niż 6 powinny zostać bezwzględnie zaktualizowane i uzupełnione o aktualny zestaw poprawek.

Outlook zostaje zainstalowany na wyraźne żądanie użytkownika jako samodzielny produkt bądź jako element pakietu Microsoft Office. Wśród wersji Outlooka dla Microsoft Windows należy wymienić:

- Outlook 95
- Outlook 97
- Outlook 98
- Outlook 2000, znany też pod nazwą Outlook 9
- Outlook XP, znany też pod nazwą Outlook 10 lub Outlook 2002
- Outlook 2003, znany też pod nazwą Outlook 11

Wersje starsze niż Outlook 2000 nie są już wspierane przez Microsoft Corp. Zaleca się więc zdecydowanie zaktualizowanie ich jak najszybciej do jednej ze wspieranych wersji (Outlook 2003, XP lub 2000).

Do każdej wersji Outlooka powinien być zainstalowany aktualny dodatek Service Pack.

Aktualne wersje dodatków Service Pack w zależności od wersji:

- Outlook 2000 – Service Pack 3
- Outlook XP (Outlook 2002) – Service Pack 3
- do Outlooka 2003 jak dotąd nie wydano dodatku Service Pack

Aktualnie zainstalowaną wersję Outlooka rozpoznać można uruchamiając program i wybierając opcję Outlook – Informacje lub podobną z menu Pomoc.

Źródła:

Outlook Express <http://www.microsoft.com/windows/oe/>

Outlook <http://www.microsoft.com/office/outlook/>

Product Lifecycle Dates [http://support.microsoft.com/default.aspx?id=fh;\[ln\];lifeprodo](http://support.microsoft.com/default.aspx?id=fh;[ln];lifeprodo)

Microsoft Office downloads <http://office.microsoft.com/OfficeUpdate>

W9.3 Wpisy CVE/CAN

[CVE-1999-0967](#), [CVE-2000-0036](#), [CVE-2000-0567](#), [CVE-2000-0621](#), [CVE-2000-0662](#),
[CVE-2000-0753](#), [CVE-2000-0788](#), [CVE-2001-0149](#), [CVE-2001-0340](#), [CVE-2001-0538](#),
[CVE-2001-0660](#), [CVE-2001-0666](#), [CVE-2001-0726](#), [CVE-2001-1088](#), [CVE-2002-0152](#),
[CVE-2002-0685](#), [CVE-2002-1056](#)

[CAN-1999-0004](#), [CAN-1999-0354](#), [CAN-1999-1016](#), [CAN-1999-1033](#), [CAN-1999-1164](#),
[CAN-2000-0105](#), [CAN-2000-0216](#), [CAN-2000-0415](#), [CAN-2000-0524](#), [CAN-2000-0653](#),
[CAN-2000-0756](#), [CAN-2001-0145](#), [CAN-2001-0945](#), [CAN-2001-0999](#), [CAN-2001-1325](#),
[CAN-2002-0285](#), [CAN-2002-0481](#), [CAN-2002-0507](#), [CAN-2002-0637](#), [CAN-2002-1121](#),
[CAN-2002-1179](#), [CAN-2002-1255](#), [CAN-2003-0007](#), [CAN-2003-0301](#), [CAN-2004-0121](#),
[CAN-2004-0215](#), [CAN-2004-0284](#), [CAN-2004-0380](#), [CAN-2004-0501](#), [CAN-2004-0502](#),
[CAN-2004-0503](#), [CAN-2004-0526](#)

W9.4 Jak sprawdzić czy Twój system jest podatny na atak?

Wszystkie komputery z zainstalowanym Internet Explorerem mają zainstalowany Outlook Express. Systemy, w których ręcznie zainstalowano Microsoft Office, mogą zawierać także Microsoft Outlook obok programów takich jak Word, Excel, PowerPoint czy Access.

System może być podatny, jeżeli:

- a. nie jest w pełni zaktualizowany, co można zweryfikować używając MS update, lub
- b. konfiguracja zabezpieczeń jest nieprawidłowa.

W9.5 Jak się przed tym chronić?

Jest kilka możliwości konfiguracji Outlooka i/lub Outlook Express w taki sposób, by zmniejszyć ryzyko wykorzystania podatności.

Zabezpieczenie Outlooka / Outlook Express

Można podjąć kilka działań aby zabezpieczyć Outlook i/lub Outlook Express i ograniczyć ryzyko związane z bezpieczeństwem.

1. Włącz odwiedzanie strony Microsoft Update, <http://windowsupdate.microsoft.com>, oraz instalację wszelkich krytycznych poprawek do listy swoich regularnych obowiązków.
2. Wyłącz okno podglądu wiadomości, wybierając Widok – Układ i odznaczając opcję Pokaż okienko podglądu.
3. Wzmocnij zabezpieczenia odnoszące się do strefy zabezpieczeń przypisanej przychodzącej poczcie elektronicznej.
Wybierz Narzędzia – Opcje i otwórz zakładkę Zabezpieczenia. Wybierz Strefa witryn z ograniczeniami (większe bezpieczeństwo). Kliknij Zastosuj i OK.

Ochrona przed załącznikami, mogącymi zawierać złośliwy kod

Outlook 2000 (SP3), Outlook 2002 (SP1 i nowsze) oraz Outlook 2003 (wszystkie wersje) zawierają skuteczne mechanizmy ochrony przed potencjalnie groźnymi załącznikami. Domyślnie wszystkie załączniki z rozszerzeniami takimi jak .exe, .com, .vbs itp. są automatycznie blokowane. Zalecany sposób przesyłania wykonywalnych plików jako załączniki jest wykorzystywanie programu archiwizującego (np. WinZip) lub posłużenie się innym mechanizmem transportu, np. FTP czy SCP.

Pełna lista rozszerzeń blokowanych automatycznie przez Outlook znajduje się pod adresem: <http://www.microsoft.com/office/ork/2003/three/ch12/OutG07.htm>

Aby poszerzyć domyślną listę blokowanych typów plików, należy zmodyfikować rejestr:

1. kliknij Start – Uruchom – wpisz regedit – wciśnij OK
2. znajdź i wybierz następujący klucz:
 - dla Outlook 2003:
HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security
 - dla Outlook XP/2002:
HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Security

- dla Outlook 2000:
HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Security
3. W menu Edycja wybierz Nowa – Wartość ciągu
 4. Wpisz Level1Add, wciśnij Enter
 5. W menu Edycja wybierz Modyfikuj
 6. Wpisz <listę_rozszerzeń_plików>, wciśnij Enter

Uwaga: Lista_rozszerzeń_plików to lista, zawierająca rozszerzenia, które chcemy zablokować. Poszczególne elementy listy powinny być rozdzielone znakiem średnika. Na przykład, aby zablokować pliki .zip i .gif przed pojawianiem się jak załączniki listu, należy wpisać .zip; .gif

Szczegółowy opis konfiguracji blokowania załączników w Outlooku opisany jest w artykule KB837388:

<http://support.microsoft.com/?kbid=837388>

Ochrona przed spamem (niechcianą korespondencją)

Outlook 2003 zawiera skuteczną ochronę przed spamem. Aby ją skonfigurować, wybierz Akcje – Wiadomości-śmieci – Opcje wiadomości-śmieci. W zakładce Opcje znajdują się cztery przełączniki, kontrolujące poziomem agresywności filtru antyspamowego.

- Bez filtrowania – spam nie jest filtrowany
- Niskie – dość skuteczne filtrowanie; większość śmieci przenoszona jest do folderu Wiadomości-śmieci i w praktyce zapewnia małą liczbę wiadomości fałszywie sklasyfikowanych jako spam
- Wysokie – agresywne filtrowanie; odsiewa niemal wszystkie śmieci (zapisuje w folderze Wiadomości-śmieci), ale może także oznaczyć jako spam niektóre poprawne wiadomości. Jeżeli aktywna jest ta opcja, należy regularnie przeglądać folder Wiadomości-śmieci, aby wyłowić z niego wiadomości, które zostały błędnie rozpoznane jako spam
- Tylko bezpieczne listy – wyłącznie korespondencja od nadawców i domen wpisanych na listy Bezpiecznych nadawców i Bezpiecznych odbiorców będzie dostarczana. Jest to rozwiązanie najbardziej odporne na spam, ale jednocześnie wymagające czasu i wysiłku na wpisanie na odpowiednie listy wszystkich adresów, z którymi prowadzimy korespondencję.

Outlook Express i starsze wersje Outlooka nie mają skutecznych zabezpieczeń przed spamem, ale mają konfigurowalną listę zablokowanych nadawców. Jest ustawienia w Outlook Express dostępne są po wybraniu z menu Narzędzia – Reguły wiadomości – Lista zablokowanych nadawców.

Ochrona przed złośliwym kodem osadzonym w treści listu

Wiadomości email ze sformatowanym tekstem (HTML, RTF) mogą mieć zaszasty w treści złośliwy kod – inaczej niż wiadomości wyłącznie tekstowe, w których nie da się ukryć żadnego kodu. Najprostszą i najskuteczniejszą metoda ochrony przed takim złośliwym kodem jest przeglądanie wiadomości wyłącznie w postaci tekstowej. Konfiguracja takiego zachowania w Outlooku 2003 wygląda następująco: Narzędzia – Opcje, zakładka Preferencje, wciśnij Opcje e-mail, zaznacz Czytaj całą standardową pocztę jako zwykły tekst oraz Czytaj całą cyfrowo podpisaną pocztę jako zwykły tekst, wciśnij dwukrotnie OK.

Ochrona przed weryfikacją adresów e-mail

Istnieją metody weryfikacji tego, że wysłany list został otwarty, a w związku z tym, że adres działa i jego właściciel jest potencjalnym dobrym odbiorcą spamu. Jest ona realizowana przez zawarcie w treści sformatowanej HTML wiadomości elektronicznej obrazka (zazwyczaj o rozmiarze 1x1 piksel). Wykorzystują ją powszechnie spamerzy i autorzy reklam. Oprócz informacji o otwarciu listu, technika ta dostarcza nadawcy dodatkowych informacji takich jak adres IP, język i wersja przeglądarki.

Zabezpieczenie przed nią jest możliwe w Outlook 2003: Wybierz Narzędzia – Opcje – zakładka Zabezpieczenia, kliknij Zmień ustawienia automatycznego pobierania, zaznacz Nie pobieraj automatycznie obrazów ani innej zawartości w wiadomościach e-mail (HTML) oraz Ostrzegaj mnie przed pobieraniem zawartości podczas edytowania, przesyłania dalej lub odpowiadania na wiadomości e-mail, kliknij dwukrotnie OK.

Zachowanie użytkownika

Ponieważ czynnik ludzki jest często najsłabszym ogniwem w łańcuchu zabezpieczeń, ważne jest, by korzystając z poczty elektronicznej stosować się do wskazań i tzw. dobrych praktyk.

Gdy otrzymujemy załącznik, nawet w przypadku listu od osoby, którą znamy, należy upewnić się, że został on przeskanowany programem antywirusowym – por. następny punkt „Oprogramowanie antywirusowe”.

Po otrzymaniu załącznika zapisz go w folderze innym niż Moje dokumenty, ponieważ ten właśnie folder jest najczęściej wykorzystywany przez wirusy jako katalog wyjściowy. Wybierz więc inny folder, być może nawet na innym dysku, do oddzielenia przychodzących załączników od reszty dokumentów.

Nigdy nie otwieraj załączników, których otrzymania się nie spodziewasz – nawet, jeżeli zostały przesłane przez osobę znajomą. Również dokumenty w formacie DOC czy XLS mogą zawierać prosty kod wykonywalny, który potrafi poczynić szkody w systemie. Jeżeli musisz otworzyć załącznik w którymś z programów Microsoft, na przykład w Wordzie, najpierw upewnij się, że ustawienia tego programu odnośnie makr są bezpieczne – otwórz Narzędzia – Opcje – Zabezpieczenia – Bezpieczeństwo makr i zaznacz opcję Wysokie, aby zapobiec wykonywaniu niepodpisanych makr.

Zawsze sprawdzaj podpisy cyfrowe plików wykonywalnych o ile tylko są one dostępne. W ten sposób możesz zweryfikować integralność pliku oraz jego pochodzenie ze sprawdzonego źródła.

Oprogramowanie antywirusowe

Oprogramowanie antywirusowe może chronić komputer przed działaniem wirusów, robaków, koni trojańskich i innych rodzajów złośliwego oprogramowania. Kluczową kwestią jest aktualizacja danych oprogramowania, która powinna odbywać się nie rzadziej niż raz w tygodniu (a najlepiej codziennie w sposób automatyczny). W ten sposób ochrona działać będzie także przed najnowszymi przypadkami zagrożeń. Większość nowoczesnych pakietów antywirusowych pozwala na wykonywanie tej czynności automatycznie. Warto także skonfigurować program tak, by skanowane były wszystkie pliki, niezależnie od ich typu i pochodzenia.

Większość pakietów antywirusowych ma możliwość przeglądania całej wychodzącej i przychodzącej poczty oraz blokowania plików ze złośliwym kodem, zanim będą miały możliwość wyrządzenia szkód w systemie.

Zdecydowanie zaleca się zainstalowanie zaktualizowanego programu do ochrony antywirusowej przed korzystaniem z poczty elektronicznej i innych usług internetowych, ponieważ wiele wirusów rozprzestrzenia się jako załączniki listów e-mail lub złośliwy kod zaszyty w treści wiadomości i wykonywany w trakcie jej czytania lub podglądu.

Źródło:

Microsoft Antivirus Reference

<http://www.microsoft.com/security/protect/antivirus.asp>

Aktualizacja Outlooka i Outlook Express

Outlook Express był w ciągu ostatnich lat kilkakrotnie uaktualniany. Za każdym razem poprawiano jego funkcjonalność, stabilność i bezpieczeństwo. Najnowsza wersja dostępna jest bezpłatnie pod adresem: <http://www.microsoft.com/windows/oe/>

Aby sprawdzić, czy używasz aktualnej wersji Outlooka i innych programów z pakietu Office, odwiedź witrynę [Office Product Updates](#). Na tej stronie zostaną automatycznie wykryte wszelkie krytyczne oraz zalecane poprawki, które należy zainstalować.

Szczegółowe informacje o cechach i ustawieniach zabezpieczeń w Office 2003 zawiera dokument [Office 2003 Security white paper](#).

Uwaga: Należy skontaktować się z administratorem sieci w firmie zanim wprowadzi się jakiegokolwiek zmiany w systemie centralnie zarządzanym. Administrator może znaleźć szczegółowe informacje techniczne o poprawkach bezpieczeństwa Outlooka tutaj: [Office Resource Kit](#).

Odinstalowanie Outlooka i Outlook Express

Jeżeli w systemie używany jest inny klient poczty elektronicznej lub menedżer osobisty, można spokojnie usunąć Outlooka i/lub Outlook Express.

Outlook we wszystkich wersjach Windows

Outlook może zostać usunięty z systemu przez otwarcie Start – Ustawienia – Panel sterowania i wybranie Dodaj/Usuń programy. Po otwarciu okienka, należy wybrać z listy Microsoft Outlook i kliknąć przycisk Usuń.

Outlook Express w Windows 98/ME

Outlook Express może zostać usunięty z systemu przez otwarcie Start – Ustawienia – Panel sterowania i wybranie Dodaj/Usuń programy. Po otwarciu okienka, należy wybrać Dodaj/Usuń składniki systemu Windows i odznaczyć z listy program Microsoft Outlook Express. Następnie należy kliknąć Zastosuj i OK, aby wprowadzić zmiany i odinstalować Outlook Express.

Outlook Express w Windows 2000/XP lub wraz z nową wersją Internet Explorer

Odinstalowanie Outlook Express w Windows 2000/XP oraz w przypadku użytkowników, którzy zaktualizowali przeglądarkę Internet Explorer jest znacznie bardziej złożone. Szczegóły postępowania opisane są w przewodnikach Microsoft:

Windows 2000 i Microsoft Outlook Express w wersji 5.x/6.0

<http://support.microsoft.com/default.aspx?scid=kb;PL-PL;q263837>

Windows 98/Me i Microsoft Outlook Express w wersji 5.x/6.0

<http://support.microsoft.com/default.aspx?scid=kb;PL-PL;q256219>

Uwaga: Outlook Express może zostać ponownie zainstalowany bez informacji o tym w przypadku instalacji service packu, pakietu poprawek krytycznych lub niektórych poprawek do systemu Windows.

[przejdź do początku dokumentu ^](#)

W10 Komunikatory IM

W10.1 Opis

Obsługa wiadomości błyskawicznych dojrzała przez ostatnich kilka lat od statusu nowinki, pozwalające na utrzymywanie kontaktu z przyjaciółmi i rodziną do ważnego składnika systemu operacyjnego Windows, używanego często do komunikacji, współpracy i wsparcia. Mimo, że komunikatory firm trzecich wciąż mają ogromny udział w rynku, uwydatnia się trend integracji narzędzi do przesyłania wiadomości błyskawicznych (IM) z systemem operacyjnym, co stwarza zagrożenie dla firm, których polityki bezpieczeństwa i regulaminy zabraniają korzystania z takiego oprogramowania. Luki wykrywane w komunikatorach stwarza także ryzyko dla firm, którym brak jest środków technicznych, wyszkolonego personelu i możliwości uporańia się z kolejnym zagrożeniem.

Obecnie znaczącą większość komunikatorów w systemach Windows stanowią Yahoo! Messenger (YM), AOL Instant Messenger (AIM), MSN Messenger (MSN) oraz Windows Messenger (WM) obecnie całkowicie zintegrowany z systemami Windows XP Professional i Home Edition. Możliwości ukryte w komunikatorach sięgają daleko poza zwykłe tekstowe przesyłanie krótkich wiadomości - od sprawdzania poczty, przez rozmowę głosową, komunikację wideo po przesyłanie i udostępnianie danych. Wyraźny jest także trend do tworzenia komunikatorów obsługujących wiele sieci i protokołów, udostępniając jeden interfejs do komunikacji, np. Miranda.

Możliwe do zdalnego wykorzystania luki w komunikatorach lub związanych z nimi bibliotekach stanowią coraz większe zagrożenie dla integralności i bezpieczeństwa sieci, wprost proporcjonalnie do ich szybkiego rozwoju i integrowania się z systemem operacyjnym. Scenariusze ataków związanych z IM są rozmaite - np. przepełnienie bufora (przez RPC lub spreparowane pakiety), ataki z wykorzystaniem złośliwych adresów URI, transferu plików i ActiveX.

Luki w komunikatorach należą zwykle do jednej z następujących kategorii:

- Błędne kontrolki ActiveX - np. przepełnienie bufora w MSN Messenger „ResDLL” CAN-2002-0155, przepełnienie bufora kontrolki ActiveX Yahoo! Voice Chat (<http://www.securityfocus.com/bid/7561>), nadpisanie bufora kontrolki ActiveX Yahoo! Webcam (<http://www.securityfocus.com/bid/8634>)
- Problemy w implementacji URI - np. wykonywanie złośliwego kodu w Yahoo! Messenger CAN-2002-0032, przepełnienie bufora obsługi URI Yahoo! Messenger CAN-2002-0031
- Różne przepełnienia bufora, np. związane z transferem plików - np. błąd walidacji pliku MSN Messenger CAN-2004-0122, błędy przepełnienia bufora pól „Imvironment” i „message” CAN-2002-0320, błąd parsowania pakietów TLV 0x2711 AOL Instant Messenger CAN-2002-0005, VU#912659, Yahoo! Messenger YAuto.DLL Open Buffer Overflow Vulnerability (<http://www.securityfocus.com/bid/9145>), AOL Instant Messenger Getfile Screenname Buffer Overrun Vulnerability (<http://www.securityfocus.com/bid/8825>)
- Komunikacja RPC - np. przepełnienie bufora spreparowaną wiadomością RPC w MSN Messenger CAN-2003-0717

Komunikatory wprowadzają nie tylko podatności sieciowe, ale także ryzyko związane z ochroną własności intelektualnej, poufnością danych, a także produktywnością pracowników. Niezależnie od uporania się z dającymi się wykorzystać zdalnie błędami w oprogramowaniu, ważne jest także stworzenie odpowiednich zapisów w regulaminach korzystania z sieci oraz wprowadzenie filtrowania ruchu wchodzącego i wychodzącego z sieci, aby uniknąć problemów związanych z obecnością w sieci komunikatorów IM.

W10.2 Podatne systemy operacyjne

Komunikatory IM mogą działać w systemach Windows 98, Windows ME, Windows 2000 w tym Professional, Windows XP oraz Windows 2003. We wszystkich wersjach Windows XP Windows Messenger jest instalowany jako część systemu operacyjnego.

W10.3 Wpisy CVE/CAN

CVE-2002-0005, CVE-2002-0032, CVE-2002-0155, CVE-2002-0785

CAN-2002-0031, CAN-2002-0228, CAN-2002-0320, CAN-2002-0362,
CAN-2003-0717, CAN-2004-0043, CAN-2002-1486

W10.4 Jak sprawdzić czy Twój system jest podatny na atak?

Aby sprawdzić numer wersji Microsoft Instant Messengera, uruchom aplikację i wybierz opcję Informacje z menu Pomoc. Wersje starsze niż 6.2 powinny zostać jak najszybciej zaktualizowane i uzupełnione o niezbędne poprawki.

W10.5 Jak się przed tym chronić?

1. Upewnij się, że wykorzystywany komunikator jest w aktualnej wersji i ma zainstalowane wszelkie dostępne poprawki.
2. Upewnij się, że w systemie zainstalowana jest poprawka MS 03-043, usuwająca lukę przepełnienia bufora w usłudze Poślaniec (Messenger).
3. Skonfiguruj system IDS/IPS tak, by wykrywał transfery plików dokonywane przy użyciu komunikatorów.
4. Jeżeli pozwala na to polityka bezpieczeństwa, zablokuj na firewallu odpowiednie porty. Zwróć uwagę, że nie rozwiąże to problemu całkowicie, ponieważ niektóre komunikatory potrafią omijać ograniczenia firewalla.
 - TCP/1863: Microsoft .NET Messenger, MSN Messenger
 - TCP/5050: Yahoo! Messenger
 - TCP/6891: MSN Messenger (transfer plików)
 - TCP/5190-5193: AOL Instant Messenger
5. Zablokuj dostęp do stron, zawierających linki URI typu "aim:" lub "ymsgr:". Może to zapobiec wykorzystaniu błędów w przetwarzaniu tych adresów. Innym rozwiązaniem jest usunięcie odpowiednich kluczy w "HKEY_CLASSES_ROOT".
6. Zablokuj dostęp do stron, zawierających kontrolki ActiveX związane z jakimkolwiek opisanym wyżej problem komunikatorów. Może to zapobiec wykorzystaniu jednej z luk w ActiveX, związanych z komunikatorami IM.

[przejdź do początku dokumentu ^](#)

Najczęstsze luki w systemach UNIX (U)

U1 Serwer nazw BIND

U1.1 Opis

Berkeley Internet Name Domain (BIND) jest najczęściej wykorzystywaną implementacją Domain Name System (DNS), krytycznego systemu pozwalającego na konwersję nazw (np. www.sans.org) na zarejestrowany numer IP. Rozpowszechnienie i krytyczność BIND sprawiły, że często stawała się ona celem ataków, w szczególności ataków Denial of Service (DoS). Ich efektem była utrata dostępu do Internetu przez wiele hostów i usług. Chociaż twórcy BIND zawsze szybko naprawiali błędy, w sieci nadal znajduje się wiele przestarzałych, źle skonfigurowanych i/lub podatnych serwerów.

Istnieje szereg przyczyn takiego stanu rzeczy - przede wszystkim nieświadomi istnienia łat bezpieczeństwa administratorzy, systemy, które mają uruchomione serwery BIND (znane pod nazwą „named”) zupełnie niepotrzebnie, oraz różne błędy w konfiguracji. W rezultacie może dojść do ataków Denial of Service, przepełnienia bufora bądź zatrucia pamięci podręcznej serwera DNS (*DNS cache poisoning*). Wśród najnowszych słabości systemu BIND znajduje się podatność na atak Denial of Service, opisana w zaleceniu [CERT CA-2002-15](#). W tym przypadku atakujący, aby wymusić wewnętrzną kontrolę poprawności, może wysłać odpowiednie pakiety DNS. Kontrola ta jest przeprowadzana błędnie, powodując zamknięcie serwera. Inny przypadek to atak przepełnienia bufora, opisany w zaleceniu [CERT Advisory CA-2002-19](#), w którym atakujący wykorzystuje luki w implementacjach bibliotek rozwiązywania nazw DNS (DNS resolver libraries). Poprzez wysyłanie złośliwych odpowiedzi DNS, atakujący może wykorzystać te luki i wykonać dowolny kod. Może także spowodować atak Denial of Service.

Istnieje również dodatkowe ryzyko związane z wykorzystaniem podatnego serwera BIND do przechowywania na nim nielegalnych materiałów bez wiedzy administratora lub jako odskoczni do dalszych ataków.

U1.2 Podatne systemy operacyjne

Prawie wszystkie wersje systemów UNIX oraz Linux są rozprowadzane z którąś z wersji BIND. BIND jest prawdopodobnie zainstalowany, jeżeli skonfigurowano system jako serwer. Istnieją też binarne wersje BIND na systemy Windows.

U1.3 Wpisy CVE/CAN

[CVE-1999-0009](#), [CVE-1999-0024](#), [CVE-1999-0184](#), [CVE-1999-0833](#), [CVE-1999-0837](#), [CVE-1999-0835](#), [CVE-1999-0849](#), [CVE-1999-0851](#), [CVE-2000-0887](#), [CVE-2000-0888](#), [CVE-2001-0010](#), [CVE-2001-0011](#), [CVE-2001-0012](#), [CVE-2001-0013](#)

[CAN-2002-0029](#), [CAN-2002-0400](#), [CAN-2002-0651](#), [CAN-2002-0684](#), [CAN-2002-1219](#), [CAN-2002-1220](#), [CAN-2002-1221](#), [CAN-2003-0914](#)

U1.4 Jak sprawdzić czy Twój system jest podatny na atak?

Jeżeli masz wersję BIND, otrzymaną wraz z systemem operacyjnym, zweryfikuj czy jesteś na bieżąco z łatami wydawanymi przez producenta systemu. Jeżeli wykorzystujesz wersję BIND skompilowaną ze źródeł udostępnionych przez [Internet Software Consortium \(ISC\)](#), upewnij się, że jest to najnowsza wersja BIND. Niezaktualizowane bądź przestarzałe wersje BIND prawdopodobnie zawierają luki, czyniące je podatnymi na atak.

W przypadku większości systemów, polecenie “named -v” wyświetli wersję zainstalowanego BIND, w postaci X.Y.Z, gdzie X jest główną wersją, Y - poboczną, a Z - wersją łaty. Obecnie istnieją trzy główne wersje BIND: 4, 8 i 9. Jeżeli masz wersję

BIND skompilowaną ze ściągniętych źródeł, powinieneś wymienić wersję 4 na wersję 9. Najnowsze źródła wersji 9.3.0rc są do pobrania ze strony [ISC](#).

Bardziej aktywną formą utrzymania należytego poziomu bezpieczeństwa BIND jest subskrypcja raportów dotyczących ostrzeżeń i luk, na przykład ze stron [SANS](#) lub [OSVDB](#). Uaktualniony skaner podatności może być bardzo skutecznym narzędziem do sprawdzania poziomu bezpieczeństwa systemów DNS.

U1.5 Jak się przed tym chronić?

- **Ogólne zalecenia dotyczące ochrony przed lukami w BIND:**
 1. Wyłącz demon BIND (zwany "named") na każdym systemie, który nie został wyznaczony i upoważniony do pełnienia funkcji serwera DNS.
 2. Zainstaluj wszystkie łaty producenta, lub uaktualnij swój serwer do najnowszej wersji. Aby uzyskać więcej informacji o zabezpieczeniu Twojej instalacji BIND, zapoznaj się z artykułami wymienionymi w dokumencie CERT, [UNIX Security Checklist](#).
 3. Zautomatyzowane ataki bądź skany Twoich systemów można utrudnić. W tym celu ukryj wersję BIND poprzez zmianę wskazania "Version String" z prawdziwej wersji na wymyśloną. Możliwość ta jest dostępna jako opcja w pliku „named.conf”.
 4. Pozwalaj na transfer stref tylko do *secondary serwerów* DNS dla Twojej domeny. Wyłącz transfery do domen nadrzędnych i poddomen, wykorzystując w zamian delegacje i forwarding.
 5. Aby uchronić skompromitowanego "named" od wystawienia całego Twojego systemu operacyjnego na atak, uruchom serwer BIND tak, by właścicielem procesu był nieuprzywilejowany użytkownik, a serwer działał w środowisku *chroot*. W tym celu, w przypadku BIND 9, zapoznaj się z <http://www.losurs.org/docs/howto/Chroot-BIND.html>.
 6. Wyłącz rekurencję i *glue fetching* aby chronić się przed atakami DNS *cache poisoning*.
- **Aby chronić się przed niedawno odkrytymi lukami w BIND:**
 1. W przypadku luki Denial of Service w ISC BIND 9: <http://www.cert.org/advisories/CA-2002-15.html>
 2. W przypadku wielu nowych luk denial of service w ISC BIND 8: <http://www.isc.org/products/BIND/bind-security.html>
 3. *Cache poisoning* poprzez negatywne odpowiedzi - <http://www.kb.cert.org/vuls/id/734644>

Bardzo dobre wskazówki zabezpieczenia BIND na systemach Solaris oraz dodatkowe odnośniki do dokumentacji BIND znajdują się w dokumencie [Running the BIND9 DNS Server Securely](#), oraz w archiwum artykułów dotyczących bezpieczeństwa BIND, dostępnych na serwerze [Afentis](#). Warto się także zapoznać z dokumentacją dostępną na stronie:

http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf

Można także rozważyć inne rozwiązania niż BIND, takie jak DJBDNS – opis na stronie: <http://cr.yip.to/djbdns.html>

[przejdź do początku dokumentu ^](#)

U2.1 Opis

Protokół HTTP jest bezsprzecznie najpopularniejszym zastosowaniem publicznego Internet. Serwery HTTP dla Unixa, takie jak Apache oraz Sun Java System Web Server (wcześniej iPlanet) obsługują większość ruchu HTTP i w związku z tym zasługują na szczególnie baczną obserwację z punktu widzenia bezpieczeństwa. Dotyczy to zarówno luk w samych serwerach, jak i w dodatkowych modułach, a także domyślnych, przykładowych i testowych stronach i skryptach, błędów w PHP oraz rozmaitych innych ataków.

Mimo, że istnieje wiele sposobów atakowania serwera WWW, najczęstszą przyczyną skutecznych ataków jest system, który nie został prawidłowo skonfigurowany w czasie instalacji lub nie był należycie utrzymywany. Skutkiem udanych ataków może być zakłócenie lub uniemożliwienie pracy serwisu, podmiana serwowanych stron lub przejście uprawnień użytkownika root w systemie, na którym działa serwer – a także wszystko, czego można dokonać pomiędzy.

Wielu producentów i uczestników projektów open-source udostępnia zalecane sposoby konfigurowania oraz uaktualnienia do swoich produktów. Jest nadzwyczaj ważne, aby administrator serwera na bieżąco zapoznawał się z nimi. Należy zdać sobie sprawę, że większość włamań na serwery WWW jest dokonywana z użyciem dobrze znanych i szeroko dostępnych skryptów, wykorzystujących luki znane od dłuższego czasu, które producent dawno załatał, bądź zareagował na nie w inny sposób.

U2.2 Podatne system operacyjne

Wszystkie systemy UNIX posiadają możliwość uruchomienia serwera WWW. Wiele wariantów systemów Linux i UNIX dystrybuowanych jest z instalacją Apache, czasami domyślnie uruchomioną. Apache i iPlanet/Java System mogą być także uruchamiane na innych systemach operacyjnych. Dotyczy to również systemów Windows, na których prawdopodobnie podatny jest na te same luki.

U2.3 Wpisy CVE/CAN

Uwaga: Jak wspomniano, zarówno Apache jak i iPlanet/Java System mogą działać na wielu systemach. W takim przypadku użytkownik powinien przejrzeć nie tylko poniższe wpisy, lecz także wpisy z listy w sekcji W1.3.

Apache

[CVE-1999-0021](#), [CVE-1999-0066](#), [CVE-1999-0067](#), [CVE-1999-0070](#), [CVE-1999-0146](#), [CVE-1999-0172](#), [CVE-1999-0174](#), [CVE-1999-0237](#), [CVE-1999-0260](#), [CVE-1999-0262](#), [CVE-1999-0264](#), [CVE-1999-0266](#), [CAN-1999-0509](#), [CVE-2000-0010](#), [CVE-2000-0208](#), [CVE-2000-0287](#), [CAN-2000-0832](#), [CVE-2000-0941](#), [CVE-2002-0061](#), [CVE-2002-0082](#), [CVE-2002-0392](#), [CAN-2002-0513](#), [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0657](#), [CAN-2002-0682](#), [CAN-2003-0132](#), [CAN-2003-0189](#), [CAN-2003-0192](#), [CAN-2003-0254](#), [CAN-2004-0488](#), [CAN-2004-0492](#)

iPlanet/Sun Java System Web Server

[CVE-2000-1077](#), [CAN-2001-0419](#), [CAN-2001-0746](#), [CAN-2001-0747](#), [CAN-2002-0686](#), [CVE-2002-0845](#), [CAN-2002-1315](#), [CAN-2002-1316](#)

OpenSSL

[CAN-2003-0543](#), [CAN-2003-0544](#), [CAN-2003-0545](#)

PHP

[CVE-2002-0081](#), [CAN-2003-0097](#), [CAN-2004-0594](#)

inne

CAN-2004-0529, CAN-2004-0734

U2.4 Jak sprawdzić czy Twój system jest podatny na atak?

Każda instalacja serwera WWW wykonana w sposób domyślny lub niezłażana, powinna być uznana za podatną. Najlepszym sposobem na bycie na bieżąco w kwestii łat dla danego produktu jest odwiedzanie stron poświęconych bezpieczeństwu w serwisie producenta, np:

- Apache HTTP Server [Main Page & Security Report](#) (i odnośniki do [ApacheWeek](#))
- [Sun Web, Portal, & Directory Servers Download Center & BigAdmin Portal](#)
- [PHP Home Page and Downloads](#)
- [OpenSSL](#)

Każdą informacją o luce należy zająć się jak najszybciej. Czas pomiędzy publikacją takiej informacji a przygotowaniem kodu wykorzystującego lukę, a następnie powstaniem robaka, jest coraz krótszy.

Aby wspomóc proces szacowania podatności, można posłużyć się jednym z wielu dostępnych skanerów, np. [Nessus](#) czy [SARA](#) (oba open-source), albo jednym z [darmowych narzędzi](#) czy [skanerów komercyjnych](#) firmy eEye. Skanowanie powinno się wykonać na całej sieci, aby wykryć także serwery działające w sieci bez wiedzy administratora.

U2.5 Jak się przed tym chronić?

1. Upewnij się, że wszystkie serwery mają zainstalowane aktualne łaty; odnośniki do stron producentów z odpowiednimi informacjami znajdują się w sekcji U2.4
2. Wyłącz wszelkie zbędne funkcjonalności serwera. W szczególności należy zwrócić uwagę na dostęp do skryptów CGI, wsparcie php, mod_ssl oraz mod_proxy (w Apache'u). Moduły te powinny być domyślnie wyłączone, a włączane tylko jeżeli są niezbędne w danym środowisku.
 - Jeżeli zachodzi konieczność korzystania z PHP, CGI, SSI czy innych mechanizmów skryptowych, rozważ wykorzystanie suEXEC, pozwalającego na wykonywanie skryptów przez Apache'a z przywilejami użytkownika innego, niż ten należący do Apache'a
 - **Uwaga:** Mechanizm suEXEC powinien być dobrze poznany i zrozumiany przed wykorzystaniem. Nieprawidłowe użycie grozi stworzeniem nowych luk w zabezpieczeniach serwera.
 1. Dla Apache'a 1.3, zobacz <http://httpd.apache.org/docs/suexec.html>
 2. Dla Apache'a 2.0, zobacz <http://httpd.apache.org/docs-2.0/suexec.html>
3. Zabezpiecz zawartość katalogów skryptów cgi-bin i innych. Upewnij się, że wszystkie skrypty testowe i przykładowe zostały usunięte.
4. Zabezpiecz PHP:
 - Jest to odrębny, szeroki temat. Poniższe uwagi to jedynie dobry punkt wyjścia do zapewnienia bezpieczeństwa instalacji PHP.
 - Wyłącz parametry, nakazujące PHP umieszczanie w nagłówkach HTTP dodatkowych informacji o systemie.

- Zapewnij działanie PHP w trybie bezpiecznym (safe mode)

Szczegółowe informacje znaleźć można na stronie
<http://www.securityfocus.com/printable/infocus/1706>

5. Istnieją dodatkowe moduły, które mogą pomóc w zabezpieczeniu serwera Apache. Moduł `mod_security` (www.modsecurity.org) pomaga w zabezpieczeniu się przed technikami Cross Site Scripting (XSS) i SQL injection. Szczegółowe informacje o instalacji i wykorzystaniu modułu znajdują się na podanej stronie.
6. Ważny jest także audyt skryptów pod kątem luk umożliwiających wykonanie ataków XSS i SQL injection. Powstało kilka narzędzi do tego właśnie celu. Jednym z najbardziej rozbudowanych skanerów słabości CGI jest Nikto (<http://www.cirt.net/code/nikto.shtml>).
7. Powinno się rozważyć uruchomienie serwera HTTP w środowisku `chroot`. W takim środowisku serwer nie ma dostępu do systemu plików poza wyznaczonymi ramami `chroot`. W ten sposób można zapobiec wykonywaniu skryptów wykorzystujących luki. Na przykład, skrypt taki mógłby odwoływać się do powłoki, a ponieważ `/bin/sh` najprawdopodobniej nie znajdzie się (a przynajmniej nie powinna się znaleźć) w środowisku `chroot`, wywołanie to nie odniesie skutku.
Uwaga: stworzenie dla serwera WWW środowiska `chroot` może nieść ze sobą efekty uboczne dla działania skryptów PHP, CGI, baz danych i modułów, które mogą wymagać od serwera dostępu do zewnętrznych bibliotek i plików wykonywalnych.
Ponieważ jest wiele sposobów tworzenia środowiska `chroot`, należy zapoznać się z dokumentacją oprogramowania.
 - <http://www.w3.org/Security/Faq/wwwsf3.html#SVR-Q5>
 - <http://www.modsecurity.org/documentation/apache-internal-chroot.html>
 - http://www.sun.com/software/whitepapers/webserver/wp_ws_security.pdf
8. Nie uruchamiaj serwera jako użytkownik z przywilejami `roota`. Na potrzeby serwera powinien być utworzony osobny użytkownik i osobna grupa z minimalnymi przywilejami, a żaden inny proces nie powinien być uruchamiany przez tego użytkownika (np. Apache powinien być uruchamiany przez użytkownika "apache", a nie "nobody").
9. Ogranicz informacje, jakie są ujawniane o wersji/konfiguracji serwera. Ta sugestia czasami wywołuje sprzeciw tych, którzy uważają, że bezpieczeństwa nie da się osiągnąć za pomocą ukrywania informacji (*security by obscurity*), a ataki i tak są przeprowadzane na ślepo (co jest łatwe do zauważenia, gdyż w wielu logach Apache'a można zobaczyć ślady exploitów na serwerach IIS). Jednak istnieją także exploity, które uruchamiają atak dopiero po sprawdzeniu nagłówka serwera.
 - Zmodyfikuj domyślny token Apache HTTP wysyłany w odpowiedzi:
 1. Dla Apache 1.3.x, zobacz <http://httpd.apache.org/docs/mod/core.html#servertokens>
<http://httpd.apache.org/docs/mod/core.html#serversignature>.
 2. Dla Apache 2.0.x, zobacz <http://httpd.apache.org/docs-2.0/en/mod/core.html#servertokens>.
 - Zadbaj o to, by moduł `mod_info` nie był osiągalny z Internetu.
 - Indeksowanie katalogów powinno być wyłączone.
10. Wydajne i staranne logowanie jest niezbędne aby skutecznie wykrywać potencjalne problemy bezpieczeństwa lub wyjaśnić nieoczekiwane zachowanie

serwera. Do dobrej praktyki należy rutynowa rotacja logów i archiwizacja starszych logów. Dzięki temu, wielkość logów nie stanie się przeszkodą w zarządzaniu serwerem. Łatwiej jest je w razie czego przeszukać. Różne informacje dotyczące formatów logów i ich rotacji dostępne są na stronach:

- o Dla Apache 1.3.x: <http://httpd.apache.org/docs/logs.html>
- o Dla Apache 2.0.x: <http://httpd.apache.org/docs-2.0/logs.html>

W wielu przypadkach zawartość logów może okazać się niewystarczająca. W szczególności, jeżeli wykorzystujesz PHP, CGI bądź inne skrypty, warto rejestrować zawartości pola danych zapytań GET i POST. Logi takie mogą dostarczyć ważnych danych oraz dowodów w wypadku włamania. Logowanie pól danych zapytań GET i POST można zaimplementować za pomocą modułu `mod_security`.

- o <http://www.modsecurity.org>
- o <http://www.securityfocus.com/infocus/1706>

[przejdź do początku dokumentu ^](#)

U3 Uwierzytelnienie

U3.1 Opis

Hasła i kody bezpieczeństwa wykorzystywane są niemal w każdym przypadku interakcji pomiędzy użytkownikiem i systemem informatycznym. Większość form uwierzytelnienia użytkownika, podobnie jak ochrony danych i plików opiera się na hasle podawanym przez użytkownika. Ponieważ prawidłowo przeprowadzone uwierzytelnienie często nie jest odnotowywane (a nawet jeśli zostaje odnotowane, zazwyczaj nie wzbudza podejrzeń), przejęte hasło użytkownika to doskonała okazja do rozpoznania systemu od wewnątrz w sposób niemal niezauważalny. Atakujący, posługując się takim hasłem, zapewnia sobie dostęp do wszelkich zasobów udostępnionych użytkownikowi oraz znajduje się znacznie bliżej możliwości penetracji innych kont w systemie, maszyn w sąsiedztwie czy przejęcia uprawnień administratora. Pomijając powyższe zagrożenie, konta ze słabymi lub pustymi hasłami pozostają wciąż na porządku dziennym, a organizacje z wdrożoną dobrą polityką dotyczącą haseł pozostają rzadkością.

Najczęstsze luki związane z hasłami to: (a) konta użytkowników ze słabymi bądź pustymi hasłami; (b) konta użytkowników z powszechnie znanymi, bądź otwarcie wystawianymi hasłami; (c) konta na poziomie administratora systemu lub aplikacji, z powszechnie znanymi, słabymi bądź pustymi hasłami; oraz (d) słabe bądź powszechnie znane algorytmy generujące skróty haseł, i/lub skróty haseł przechowywane bez należytej ochrony, do odczytu dla wszystkich.

Najlepszą ochroną przed tymi zagrożeniami jest dobrze zdefiniowana polityka zarządzania hasłami, uwzględniająca dokładne instrukcje dla użytkowników: jak stworzyć silne hasło, jak zadbać o ich poufność, a także określenie zasad postępowania personelu IT w zakresie szybkich zmian słabych/niebezpiecznych/domyślnych bądź powszechnie znanych haseł, i szybkiego zamykania nieużywanych kont oraz regularne sprawdzanie wszystkich haseł pod kątem ich odporności na złamanie. Warto zapoznać się z "General Unix configuration guide" dostępnego na stronach: http://www.cert.org/tech_tips/unix_configuration_guidelines.html

U3.2 Podatne systemy operacyjne

Każdy system bądź aplikacja, która wymaga uwierzytelnienia użytkownika za pomocą identyfikatora i hasła.

U3.3 Wpisy CVE/CAN

[CAN-1999-0501](#), [CVE-1999-0502](#), [CAN-1999-1029](#), [CVE-2001-0259](#), [CVE-2001-0553](#), [CVE-2001-0978](#), [CVE-2001-1017](#), [CVE-2001-1147](#), [CVE-2001-1175](#), [CAN-2004-0243](#), [CAN-2004-0653](#)

U3.4 Jak sprawdzić czy Twój system jest podatny na atak?

1. Sprawdź domyślne konta

Jeżeli w systemie istnieją konta dzielone przez wielu użytkowników lub tymczasowych pracowników, albo wystawia się hasła w postaci notatek na biurkach bądź karteczkach przyczepionych do monitora, to konta te stanowią oczywiste punkty wejścia do Twojej sieci dla każdego, kto ma fizyczny dostęp do Twoich systemów.

2. Sprawdź jakość haseł i jakość polityki zarządzania hasłami

Konfiguracja nowych kont użytkowników z tym samym lub łatwym do zgadnięcia pierwszym hasłem (nawet, jeżeli hasło to zostało zmienione po pierwszym zalogowaniu się do systemu), potencjalnie umożliwi atakującemu uzyskanie dostępu do Twoich systemów.

Sprawdź każdy system pod kątem tego, gdzie przechowywane są skróty haseł – czy w `/etc/passwd`, czy `/etc/shadow`. Plik `/etc/passwd` musi być do odczytu przez wszystkich użytkowników na systemie (tylko wtedy system może uwierzytelnić użytkownika). Jednak, jeżeli ten plik zawiera też skróty haseł, każdy użytkownik z dostępem do systemu może odczytać te skróty i spróbować je złamać za pomocą oprogramowania do łamania haseł. Plik `/etc/shadow` jest z założenia do odczytu tylko przez roota, i jeżeli to możliwe, powinien być wykorzystywany do przechowywania skrótów. Jeżeli Twoje lokalne konta nie są chronione przez `/etc/shadow`, szanse złamania Twoich haseł wzrastają. Większość nowych systemów operacyjnych domyślnie wykorzystuje `/etc/shadow`, chyba, że instalujący zdecydował inaczej. Może też istnieć możliwość zastosowania skrótów MD5. Jest to nieco bardziej bezpieczny algorytm, niż starsze algorytmy wykorzystywane przez funkcje *crypt*.

3. Środowisko NIS

NIS to zestaw usług, tworzących bazę danych (składającą się z tzw. map), świadcząca usługi informacyjne innym usługom sieciowym, jak na przykład Network File System (NFS). Pliki konfiguracyjne NIS zawierają skróty haseł NIS. Hasła te stanowią zagrożenie, ponieważ mogą zostać odczytane przez wszystkich użytkowników. Podobnie jest w przypadku niektórych implementacji LDAP, wykorzystywanych do uwierzytelnienia. Nowsze implementacje NIS, takie jak NIS+ lub LDAP, są zazwyczaj bardziej skrupulatne w ochronie skrótów haseł, chyba że instalujący zmieni domyślną konfigurację. Nowsze implementacje są bardziej skomplikowane w zainstalowaniu i konfiguracji, co czasami zniechęca do ich stosowania.

4. Ogólne zalecenia

Nawet jeżeli skróty haseł są chronione przez /etc/shadow lub inne implementacje, hasła można odgadnąć na inne sposoby. Potencjalne zagrożenie stanowią nieużywane konta byłych pracowników. Większość organizacji zaniedbuje zamykanie starych kont, chyba że zostały wprowadzone odpowiednie procedury lub administrator jest wystarczająco skrupulatny.

Domyślne instalacje (producenta lub administratora) systemów operacyjnych lub aplikacji sieciowych mogą zawierać wiele niepotrzebnych bądź niewykorzystywanych usług. Często ze względu na niepewność związaną z potrzebami danego systemu operacyjnego lub aplikacji, wielu producentów i administratorów na wszelki wypadek instaluje wszystko. Upraszcza to procedurę instalacyjną, ale wprowadza też wiele niepotrzebnych usług i kont z domyślnymi, słabymi bądź znanymi hasłami.

Dodatkowo, hasła przesyłane tekstem jawnym, za pomocą protokołów takich jak telnet, FTP lub HTTP są podatne na podsłuch. Aby ograniczyć taką możliwość, wskazane jest wykorzystanie zaszyfrowanych połączeń, za pomocą rozwiązań takich jak OpenSSH lub SSL.

U3.5 Jak się przed tym chronić?

Najlepszą i najbardziej stosowną ochroną przed słabymi hasłami jest silna polityka zarządzania hasłami, która zawiera szczegółowe instrukcje w zakresie nauczania użytkownika dobrych zwyczajów zarządzania hasłami, a także uwzględnia sprawdzanie integralności haseł przez administratorów, udzielając im pełnego poparcia kierownictwa organizacji. Aby stworzyć dobrą politykę w tym zakresie, należy podjąć następujące kroki:

1. **Zadbaj o silne hasła.** Posiadając wystarczającą ilość sprzętu i czasu, każde hasło może być złamane za pomocą ataku brutalnego. Oprogramowanie łamiące hasła (*password crackers*), często wykorzystywane przez atakujących, wykonuje atak słownikowy. Ponieważ najpowszechniejsze algorytmy szyfrowania haseł są znane, narzędzia te po prostu porównują skrót wszystkich słów w słowniku (w wielu językach), a także imion, oraz ich różnych permutacji, ze skrótem hasła. Tak więc, każde hasło które przypomina jakiś wyraz (w dowolnym języku), jest podatne na atak słownikowy. Wiele organizacji zachęca użytkowników do tworzenia haseł z uwzględnieniem znaków alfanumerycznych i specjalnych. W konsekwencji użytkownicy biorą jakiś wyraz (np.: *password*) i zmieniają litery na cyfry bądź znaki specjalne (np.: *pa\$\$w0rd*). Takie permutacje nie chronią przeciwko atakowi słownikowemu: prawdopodobieństwo złamania *pa\$\$w0rd* jest podobne do prawdopodobieństwa złamania *password*.

Dobre hasło nie może pochodzić od wyrazu lub imienia. Silna polityka zarządzania hasłami powinna nakazywać użytkownikom generowanie hasła z czegoś bardziej losowego, jak na przykład fraza, dłuższy tytuł książki bądź piosenki. Poprzez złączenie dłuższej frazy w hasło (na przykład, branie pierwszej litery każdego wyrazu we frazie, używając wielkie i małe litery, lub podmiana znaku specjalnego zamiast słowa, i/lub zamiana wszystkich samogłosek na znaki specjalne w tak stworzonym hasle), użytkownicy mogą wygenerować odpowiednio długie hasła, z odpowiednimi kombinacjami znaków alfanumerycznych i znaków specjalnych, w sposób utrudniający ich złamanie

metodą ataku słownikowego. A jeżeli pierwotną frazę było łatwo zapamiętać, to samo powinno dotyczyć hasła.

Po udostępnieniu użytkownikom odpowiednich instrukcji, dotyczących tworzenia dobrych haseł, powinno się opacać szczegółowe procedury w celu upewnienia się, czy instrukcje te są przestrzegane. Większość odmian UNIXa/Linuxa może wykorzystać Npasswd jako front-end do sprawdzania zgodności wprowadzanych haseł z polityką bezpieczeństwa. Systemy, które mają wsparcie dla PAM mogą także wykorzystać biblioteki cracklib (udostępniane wraz z programem Crack) do sprawdzania haseł podczas ich generacji. Większość systemów z PAM-em można też skonfigurować tak, aby odrzucały hasła, które nie są zgodne z polityką.

Jeżeli jednak hasła nie mogą być sprawdzane za pomocą bibliotek słownikowych (przez Npasswd bądź biblioteki PAM), administrator w ramach procedury powinien regularnie uruchamiać narzędzia do łamania haseł. W tym celu najlepiej wykorzystać narzędzia potencjalnych atakujących. Na systemach UNIX/Linux do tych narzędzi należą Crack i John the Ripper.

Uwaga: Nigdy nie uruchamiaj narzędzia do łamania haseł, nawet na systemach, na których masz uprawnienia root, bez wyraźnej zgody kierownictwa/pracodawcy, najlepiej na piśmie. Zdarzało się, że administratorów, którzy mieli jak najlepsze intencje, zwalniano za działanie bez pozwolenia. Pozwolenie to powinno być w postaci listu, i tworzyć część polityki zarządzania hasłami organizacji, która zezwala na okresowe sprawdzanie jakości haseł.

Kiedy już masz pozwolenie do łamania haseł na Twoim systemie, rób to regularnie na odpowiednio zabezpieczonym, również fizycznie, systemie. Użytkownicy, którym złamano hasło, powinni zostać powiadomieni dyskretnie, a następnie poinstruowani, jak lepiej dobierać hasła. Procedury powiadamiania użytkowników w takich przypadkach powinny być opracowane wspólnie przez administratorów i kierownictwo organizacji, jako część polityki zarządzania hasłami tak, aby kierownictwo zapewniło wsparcie w sytuacji, w której użytkownicy nie reagują na uwagi administratorów.

Inne możliwości w zakresie ochrony przed pustymi bądź słabymi hasłami i/lub utrzymywania polityki zarządzania hasłami to (a) wykorzystanie innych form uwierzytelnienia - tokeny generujące hasła, biometria. Sposoby te są skuteczne, jeżeli masz problemy ze słabymi hasłami, a jednocześnie posiadasz możliwość alternatywnej metody uwierzytelniania użytkowników. Warto zwrócić uwagę na fakt, że niektóre tokeny wymagają procedur w zakresie ich ochrony przed nieupoważnionymi użytkownikami, i w przypadku kradzieży powinny zostać zablokowane w systemie. Biometria to rozwijająca się dziedzina i w zależności od metody uwierzytelnienia (np.: na podstawie odcisków palców lub rozpoznawania twarzy), niektóre metody nie zostały jeszcze dopracowane, mogą więc zdarzać się dość częste pomyłki. (b) Istnieje wiele dobrych narzędzi (zarówno darmowych jak i odpłatnych), które można wykorzystać do zarządzania hasłami.

2. **Chroń silne hasła:** Jeżeli przechowujesz skróty haseł w /etc/passwd, uaktualnij swój system tak, aby korzystał z /etc/shadow. Jeżeli system wykorzystuje NIS lub LDAP w sposób uniemożliwiający ochronę haseł, każdy, nawet nieuwierzytelniony użytkownik może odczytać skróty haseł i spróbować je złamać. Należy poszukać bezpieczniejszej alternatywy w stosunku do wykorzystywanych wersji NIS i LDAP. Dopóki te niebezpieczne aplikacje nie zostaną zabezpieczone lub wymienione, należy regularnie, w ramach odpowiedniej procedury i po uzyskaniu pozwolenia, sprawdzać jakość ich haseł. Warto, zamiast tradycyjnego crypt, wziąć pod uwagę algorytm MD5 do generacji skrótów haseł.

Nawet jeśli hasła same w sobie są dość silne, konta do których są przypisane mogą zostać przejęte, jeżeli hasła te nie będą należycie chronione przez użytkowników. W dobrze skonstruowanej polityce powinny zostać uwzględnione zakazy udostępniania hasła innym osobom, zapisywania ich w sposób umożliwiający niepowołany dostęp do nich i nakaz należytego zabezpieczenia plików zawierających hasła służące do automatycznego uwierzytelnienia (w istocie dużo łatwiej jest chronić hasła, gdy stosowanie takich metod uwierzytelnienia ograniczy się do przypadków absolutnej konieczności). Należy także wymusić wygasanie haseł, co sprawia, że słabe hasła, które z jakichś przyczyn nie zostały odsiane przez inne polityki, są używane jedynie przez krótki okres czasu. Starych haseł nie powinno się używać ponownie. Dobrą praktyką jest uprzedzanie użytkowników o kończącym się wkrótce okresie ważności ich hasła. Gdy na ekranie pojawia się komunikat „Twoje hasło wygasło i musi zostać zmienione”, użytkownicy będą bardziej skłonni wybrać słabe hasło.

3. **Dokładnie kontroluj konta.**

- Każde konto administratora bądź usługi, które nie jest wykorzystywane, powinno być wyłączone, a jeżeli możliwe, usunięte.
- Każde konto administratora bądź usługi, które jest wykorzystywane, powinno mieć ustanowione nowe i silne hasło, od razu po instalacji usługi/konta.
- Instaluj nowe konta użytkowników z losowo wygenerowanym hasłem wstępnym, i wymuś zmianę tego hasła przy pierwszym zalogowaniu.
- Regularnie wykonuj audyt kont na systemach, i sporządź listę wszystkich tych kont, usług wymagających istnienia tego konta i poziomu wymagań na konto.
- Opracuj dokładne procedury dodawania/usuwania upoważnionych kont do/z listy.
- Stwórz procedury usuwania kont kiedy pracownicy bądź użytkownicy kontraktowi odchodzą z pracy lub kiedy konta te nie są dalej potrzebne. Warto w tym celu nawiązać kontakt z departamentem kadr (HR).
- Regularnie sprawdzaj listę, w celu upewnienia się czy nie dodano nowych kont i, że niewykorzystywane konta zostały usunięte.

Pamiętaj też o kontaktach i hasłach na systemach takich jak routery, switchy, cyfrowe drukarki podpięte do sieci, kopiarki i serwery drukarek. Jeżeli systemy te mają słabe systemy zarządzania hasłami, a użytkownicy mają takie same hasła na tych urządzeniach oraz na systemach Unix, to powstaje dodatkowy słaby punkt.

Listę domyślnych haseł na wiele platform można znaleźć na stronie:
<http://www.cirt.net/cgi-bin/passwd.pl>

4. Szyfrowana transmisja

Wykorzystanie nawet najmocniejszych haseł nie uchroni nas przed atakiem, jeżeli hasła te przesyłane są w sieci otwartym tekstem. W takiej sytuacji każdy kto ma dostęp do kanału transmisyjnego będzie w stanie odczytać hasło. Przykładem programów i protokołów, które w ten sposób transmitują hasła to: telnet, FTP, HTTP i Berkeley "r-services".

Aby temu zapobiec, konieczne jest wykorzystanie programów i protokołów, które oferują mechanizm szyfrowania. Istnieje kilka alternatyw dla wyżej wymienionych programów: OpenSSH może zastąpić telnet, FTP i Berkeley "r-services", natomiast SSL umożliwia szyfrowanie HTTP.

5. Konta superużytkowników

Konto root jest najbardziej uprzywilejowanym kontem w systemie Unix. Zasadniczo nie ma żadnych ograniczeń w jego wykorzystaniu do dowolnej operacji na systemie. W związku z tym jest głównym celem włamywacza.

- Nie pozwalaj na zdalne bezpośrednio logowanie się na konto root. Użytkownicy powinni wykorzystać polecenie "su" do uzyskania praw roota. Polecenie "su" zmienia efektywny uid konta na inne, w tym przypadku konta roota.
- Jeżeli użytkownik potrzebuje mieć dostęp do tylko kilku uprzywilejowanych poleceń, korzystaj z sudo. Za pomocą sudo (superuser do), administrator może przydzielić użytkownikom (lub grupom użytkowników) prawa do uruchomienia niektórych (bądź wszystkich) poleceń z prawami root, jednocześnie odpowiednio zapisując te polecenia oraz ich parametry w dzienniku zdarzeń. Użytkownik nie musi w tym celu znać hasła roota.
- Korzystanie z konta root powinno być ograniczone do sytuacji konfiguracji systemu lub w sytuacjach awaryjnych.
- Należy ograniczyć dostęp do hasła root. Powinno być znane tylko osobom odpowiedzialnym za administrację systemem.

Więcej informacji na temat sudo można uzyskać na stronie:
<http://www.courtesan.org/sudo/> natomiast informacje na temu "su" można uzyskać wpisując "man su" w linii poleceń.

6. Konta domyślne

Konta domyślne są często wykorzystywane podczas tworzenia oprogramowania, tak aby rozwijana aplikacja mogła komunikować się z inną lub z bazą danych. Dostęp dla producenta to także sytuacja w której często są wykorzystywane hasła domyślne. Ważne jest odpowiednie zarządzanie takimi kontami, tak aby było wiadomo, kto z nich korzystał.

Uwagi ogólne

- Po pierwsze, należy starać się unikać korzystania z takich kont. Jeżeli dany użytkownik wymaga częstego dostępu do systemu, powinien otrzymać własne indywidualne konto.
- Jeżeli konto domyślne jest konieczne (np. wiele osób od strony producenta wymaga dostępu, albo istnieją aplikacje wymagające dostępu), należy wyznaczyć stronę odpowiedzialną za wszelkie czynności wykonywane na koncie.

Hasła aplikacji

- Nie wpisuj haseł "na sztywno" do aplikacji
- Upewnij się, że stosowane są odpowiednie zabezpieczenia informacji dotyczących kont i haseł (szyfrowane pliki, poprawne prawa dostępu itp)

Dostęp ze strony serwisanta/producenta

- Uzyskaj od producenta podpisane oświadczenie, w którym producent bierze na siebie odpowiedzialność za czynności wykonywane na koncie
- Ustal osobę ze strony producenta odpowiedzialną za zarządzaniem hasłami na kontaktach
- Przechowuj hasła dla kont serwisowych w odpowiednio zabezpieczonych kopertach, i wymagaj, aby serwisant/producent kontaktował się w celu jego uzyskania
- Korzystaj z dwu poziomowego uwierzytelnienia, jeżeli to możliwe
- Wymagaj, aby osoba od strony serwisanta/producenta zmieniała hasła po ich wykorzystaniu (może nie być konieczne, jeżeli wykorzystywane jest dwu poziomowe uwierzytelnienie).
- Regularnie sprawdzaj, czy koperty z hasłami nie zostały naruszone
- Regularnie wykonuj audyt kont

7. Audyt

Wskazane jest przechowywanie logów działań użytkowników na kontaktach. Logowanie udanych i nieudanych prób logowania się na system pozwoli zorientować się w tym co się dzieje w systemie. Poprawne logowanie wywołań sudo i su jest także niezbędne, gdyż pozwoli na wykrycie kto próbuje wykonać operacje do których nie jest upoważniony.

Częsta analiza logów pozwoli na wykrycie potencjalnych nadużyć uprawnień systemowych. Więcej informacji na temat logowania można uzyskać na stronie: <http://www.loganalysis.org>

[przejdź do początku dokumentu ^](#)

U4 Systemy kontroli wersji

U4.1 Opis

Systemy kontroli wersji to narzędzia, które służą do zarządzania zmianami dokumentów bądź kodu źródłowego i umożliwiają wielu użytkownikom równoległą pracę na tych samych zbiorach plików. Systemy takie są niezbędne do zarządzanie projektem, w którym rozwijane jest oprogramowanie, bądź tworzone są dokumenty

biznesowe i prawne, gdyż poza zapewnieniem centralnego repozytorium pozwalają na uzyskanie dostępu do różnych wersji.

Concurrent Version System (CVS) jest najpopularniejszym systemem kontroli wersji w środowisku Unix/Linux. Wiele projektów open-source udostępnia repozytoria CVS anonimowym użytkownikom. Zdalny dostęp do repozytorium CVS można skonfigurować za pośrednictwem protokołu „pserver”, domyślnie na porcie 2401/tcp. Tak skonfigurowany serwer jest podatny na kilka problemów:

- A) Przepełnienie sterty, które może zostać wywołane poprzez odpowiednio spreparowane „Entry-Lines”. Atakujący może wykorzystać przepełnienie do wykonania dowolnego kodu na serwerze CVS. Exploity na serwery CVS, uruchomionych na platformach Linux, FreeBSD i Solaris, zostały opublikowane zostały opublikowane na wielu listach dyskusyjnych. Warto zauważyć, że dowolne repozytorium które skonfigurowano z dostępem „anonymous” zawiera takie potencjalne luki.
- B) Luki w implementacjach innych poleceń i funkcji mogą zostać wykorzystane przez uwierzytelnionego atakującego do przeprowadzania ataku denial of service na serwer CVS, bądź wykonania dowolnego kodu. Część z tych luk może być także wykorzystana przez anonimowych użytkowników.

Subversion to inny system kontroli wersji na systemy Linux zyskujący coraz większą popularność. Celem projektu było stworzenie lepszego systemu od CVS. Repozytorium Subversion może być zdalnie osiągalne za pomocą protokołu „svn”, jeżeli uruchomiony został proces „svnserv”. Serwer svn domyślnie uruchomiony jest na porcie 3690/tcp. Serwer zawiera następujące luki:

- Przepełnienie sterty, które może zostać wykorzystane przez nieuwierzytelnionego atakującego do wykonania dowolnego kodu,
- Przepełnienie stosu, które może zostać wywołane przez specjalnie spreparowane polecenie svn „get-dated-rev”. Jeżeli serwer został skonfigurowany dla anonimowego dostępu, atakujący może wykonać dowolny kod na serwerze. Wiele exploitów na tę lukę opublikowano w Internecie.

Jeżeli atakujący uzyska dostęp do repozytorium, może dodać do kodu źródłowego rozwijanego oprogramowania tylne furtki i błędy, których efektem będzie wiele skompromitowanych systemów, na którym oprogramowanie zostanie w przyszłości uruchomione. Atakujący może także spróbować podszyć się pod innych pracowników, wrabiając ich w podobne zmiany.

U4.2 Podatne systemy operacyjne

Podatności dotyczą wszystkich systemów Linux, FreeBSD, AIX, HP-UX, Solaris i SGI, z uruchomionym serwerem CVS i/lub Subversion.

U4.3 Wpisy CVE/CAN

[CAN-2004-0396](#), [CAN-2004-0414](#), [CAN-2004-0416](#), [CAN-2004-0417](#), [CAN-2004-0418](#)
[CAN-2004-0397](#), [CAN-2004-0413](#)

U4.4 Jak sprawdzić czy Twój system jest podatny na atak?

Jeżeli Twój serwer CVS zezwala na zdalny dostęp za pośrednictwem protokołu „pserver” i uruchomiona jest któraś z poniższych wersji serwera, to system CVS jest podatny na atak:

CVS stable release version 1.11.16 i wcześniejsze

CVS feature release version 1.12.8 i wcześniejsze

Wersje CVS można rozpoznać poprzez polecenie „cvs ver”.

Jeżeli Twój serwer Subversion zezwala na zdalny dostęp za pośrednictwem protokołu „svn” i wersja serwera jest wcześniejsza niż 1.0.5, serwer jest podatny na atak.

U4.5 Jak się przed tym chronić?

Serwer CVS:

- Upewnij się, że serwer CVS ma zainstalowane aktualne łąty. Źródła najnowszej wersji oprogramowania są dostępne na stronie:
<https://www.cvshome.org/>
- Skonfiguruj CVS serwer dla zdalnego dostępu tak, aby korzystał z SSH a nie protokołu „pserver”. Dodatkowo, uruchamiaj serwer CVS w środowisku „chroot”. Dokładne instrukcje jak to zrobić znajdują się na stronie:
<http://www.netsys.com/library/papers/chrooted-ssh-cvs-server.txt>
- Jeżeli zdalny dostęp do repozytorium jest konieczny z poziomu sieci przedsiębiorstwa, zablokuj dostęp do portu 2401/tcp na stykach z sieciami zewnętrznymi.
- Upewnij się, że publicznie dostępne exploity nie są skuteczne przeciwko Twojemu serwerowi:
http://www.k-otik.com/exploits/05212004.CVS_Linux.c.php
http://www.k-otik.com/exploits/05212004.CVS_Solaris.c.php
- Spróbuj udostępnić repozytorium anonimowo w trybie read-only, na dedykowanym systemie (tak jak w przypadku serwerów w DMZ)

Serwer Subversion:

- Upewnij się, że serwer Subversion ma zainstalowane aktualne łąty. Źródła najnowszej wersji oprogramowania są dostępne na stronie:
<http://subversion.tigris.org>
- Skonfiguruj CVS serwer dla zdalnego dostępu tak, aby korzystał z webDAV a nie z protokołu „svn”.
- Jeżeli zdalny dostęp do repozytorium jest konieczny z poziomu sieci przedsiębiorstwa, zablokuj dostęp do portu 3690/tcp na stykach z sieciami zewnętrznymi.
- Upewnij się, że publicznie dostępne exploity nie są skuteczne przeciwko Twojemu serwerowi:
http://www.metasploit.com/projects/Framework/modules/exploits/svnserve_date.p
<http://www.k-otik.com/exploits/06112004.subexp.c.php>
- Spróbuj udostępnić repozytorium anonimowo w trybie read-only, na dedykowanym systemie (tak jak w przypadku serwerów w DMZ).

U4.6 Bibliografia

CERT Advisory

<http://www.kb.cert.org/vuls/id/192038>

SecurityFocus BIDs

<http://www.securityfocus.com/bid/10384>

<http://www.securityfocus.com/bid/10499>

<http://www.securityfocus.com/bid/10386>

<http://www.securityfocus.com/bid/10519>

Strona domowa CVS

<http://www.cvshome.org>

Strona domowa Subversion
<http://subversion.tigris.org>

Wiadomości na listach dyskusyjnych

<http://www.securityfocus.com/archive/1/363775/2004-05-17/2004-05-23/0>

<http://www.securityfocus.com/archive/1/365541/2004-06-07/2004-06-13/0>

<http://www.securityfocus.com/archive/1/363781/2004-05-17/2004-05-23/0>

<http://archives.neohapsis.com/archives/bugtraq/2004-06/0180.html>

[przejdź do początku dokumentu ^](#)

U5 Serwer pocztowy

U5.1 Opis

Email jest jedną z najczęściej wykorzystywanych usług w Internecie. Mail Transfer Agents (MTA) to serwery odpowiedzialne za dostarczenie poczty od nadawcy do odbiorcy lub odbiorców, zazwyczaj z wykorzystaniem protokołu SMTP (jeden z najstarszych protokołów Internetowych). Protokół ten może być szyfrowany za pomocą TLS, jeżeli obie strony biorące udział w transmisji mają dla niego wsparcie. Sendmail jest najczęściej wykorzystywanym MTA w systemach Unix, jednakże ze względu na fakt, że znajdowano w nim wiele luk, powstało wiele alternatywnych systemów, takich jak: Qmail, Postfix, Exim czy Courier-MTA.

E-mail jest obszarem ataku wielu wirusów, robaków i ataków polegających na „inżynierii społecznej”. Chociaż wiele z tych ataków dotyczy klientów poczty, same MTA są także często obiektem ataku. Luki obecnie wykorzystywane w systemach MTA można podzielić na następujące kategorie:

- Ataki na niezalutane systemy – przepełnienia bufora, przepełnienia sterty etc.
- Nadużycia otwartych relay – ulubione zajęcie spamerów
- Wykorzystanie innych błędów w konfiguracji – takich jak uzyskanie listy kont użytkowników na potrzeby spamu lub ataków inżynierii społecznej (a nawet ataków na klientów e-mail)

Można mieć pewność, że jeżeli w sieci znajdują się jakiś podatny serwer MTA, to zostanie szybko odnaleziony i wykorzystany w ataku. Na szczęście można drastycznie obniżyć ryzyko dla systemów MTA poprzez wykonanie kilku podstawowych kroków podczas instalacji i poprzez późniejsze odpowiednie utrzymanie serwera. MTA, które działają dokładnie zgodnie ze specyfikacją RFC są najodpowiedniejsze, gdyż większość oprogramowania do rozsyłania spamu nie jest w pełni zgodne z RFC.

U5.2 Podatne systemy operacyjne

Podatne są właściwie wszystkie systemy Unix, które są dystrybuowane z którąś z wyżej wymienionych MTA. Domyślne konfiguracje systemów Unix zostały w ciągu ostatnich kilku lat znacznie poprawione pod względem bezpieczeństwa, jednak należy przyjąć, że MTA które nie jest regularnie łątany lub działa w domyślnej konfiguracji jest podatny na atak.

U5.3 Wpisy CVE/CAN

Sendmail

[CVE-1999-0047](#), [CVE-1999-0095](#), [CVE-1999-0096](#), [CVE-1999-0129](#), [CVE-1999-0131](#), [CVE-1999-0203](#), [CVE-1999-0204](#), [CVE-1999-0206](#), [CVE-1999-1109](#), [CVE-2000-0319](#), [CVE-2001-0653](#), [CVE-2001-1349](#), [CVE-2002-0906](#)

CAN-1999-0098, CAN-1999-0163, CAN-2001-0713, CAN-2001-0714, CAN-2001-0715, CAN-2002-1165, CAN-2002-1278, CAN-2002-1337, CAN-2003-0161, CAN-2003-0285, CAN-2003-0694

Qmail

CVE-2000-0990, CAN-2003-0654

Courier-MTA

CVE-2002-0914, CVE-2002-1311, CVE-2003-0040, CVE-2004-0224, CVE-2004-0777

Exim

CVE-2001-0889

CAN-2003-0743, CAN-2004-0399, CAN-2004-0400

Postfix

CAN-2003-0468

U5.4 Jak sprawdzić czy Twój system jest podatny na atak?

Sprawdź swój patch level

Pierwszym krokiem jest sprawdzenie, jakie łaty są zainstalowane na MTA, i sprawdzenie, czy związane są z zainstalowaną wersją jakieś znane luki. W tym celu można wykorzystać CVE (cve.mitre.org).

Sendmail

W przeszłości w serwerach Sendmail znajdowano wiele luk. Wiele z nich brało się z niezwyklego stopnia skomplikowania oprogramowania. Sendmail był jedną z najczęściej atakowanych aplikacji w sieci.

Każdy przestarzały bądź niezaktualizowany Sendmail jest najprawdopodobniej podatny na atak.

Aby stwierdzić, jaka wersja Sendmaila jest zainstalowana, wykonaj następujące polecenie:

```
echo \$$Z | sendmail -bt -d
```

Nie ufaj zawsze wersji systemu wyświetlanej przez demon, gdyż jest ona czytana z pliku konfiguracyjnego, który mógł zostać niepoprawnie zaktualizowany.

Aby sprawdzić, czy masz zainstalowaną aktualną wersję Sendmaila, zajrzyj na stronę: <http://www.sendmail.org/current-release.html>

Exim

Exim jest kolejnym popularnym MTA. W przeszłości zawierał kilka luk.

Aby sprawdzić, jaka jest zainstalowana wersja Exima, należy wydać polecenie:
exim -bV

Aby sprawdzić, czy masz zainstalowaną aktualną wersję Exima, zajrzyj na stronę: <http://www.exim.org/version.html>

Qmail

Qmail jest bezpiecznym MTA, w którym nie znaleziono wiele luk. Jest jednym z najbardziej popularnych MTA, za Sendmailem.

Nie ma prostego sposobu na sprawdzenie wersji Qmaila poza sprawdzeniem wersji w podręczniku „man” za pomocą narzędzia GNU grep:
grep -A1 version /var/qmail/man/man7/qmail.7

Qmail posiada wiele ulepszeń dodawanych przez różnych użytkowników, co sprawia, że rozpoznanie luk jest dosyć skomplikowane.

Zalecane łaty można znaleźć na stronie: <http://www.qmail.org/top.html#patches>.
Można też ściągnąć pakiet netqmail, który zawiera qmail i zalecane łaty:
<http://www.qmail.org/netqmail/>

Courier-MTA

Courier-MTA jest MTA który ściśle przestrzega RFC. Zawiera wsparcie dla Maildir+, maildrop oraz MySQL, Postgres i LDAP do przechowywania aliasów i kont użytkowników.

Aby uzyskać wersje systemu, wystarczy wykorzystać polecenie „showmodules”.

Biuletyny bezpieczeństwa i informacje o aktualnej wersji można uzyskać pod adresem:
<http://www.courier-mta.org>

Postfix

Jak Qmail, Postfix jest bezpiecznym systemem MTA, i w przeszłości miał jeszcze mniej luk bezpieczeństwa. Nowsze wersje posiadają rozszerzone możliwości kontroli dostępu, sprawdzania zawartości oraz rate limiting, tak więc uaktualnienie wersji może być dobrym pomysłem, nawet jeżeli zainstalowana wersja nie zawiera luk.

Aby stwierdzić, jaka jest zainstalowana wersja, należy wydać polecenie:
postconf -d mail_version

Aby stwierdzić, jaka jest najbardziej aktualna wersja, należy odwiedzić stronę:
<ftp://ftp.porcupine.org/mirrors/postfix-release/index.html>

* Sprawdź swój relay

Pośredniczenie w przekazywaniu poczty (relay) jest podstawową funkcją MTA, jednak błędy konfiguracyjne mogą sprawić, że MTA zacznie funkcjonować jako „open relay”. W takiej sytuacji serwer MTA przekazuje pocztę nawet wtedy, kiedy ani nadawca ani odbiorca nie jest lokalnym użytkownikiem. W normalnych warunkach taka sytuacja nie powinna mieć miejsca.

Sprawdzanie, czy serwer działa w trybie „open relay”

Sprawdzanie, czy serwer działa w trybie „open relay” jest podstawową czynnością jaką należy wykonać zaraz po weryfikacji wersji systemu. Pozwoli na określenie, czy Twój serwer może zostać wykorzystany do rozsyłania spamu. W tym celu można skorzystać z następujących narzędzi:
<http://www.abuse.net/relay.html>

<http://www.cymru.com/Documents/auditing-with-expect.html>

Co to jest RBL (Realtime Blackhole List)?

RBL to lista adresów IP serwerów, których właściciele odmawiają zablokowania przypadków rozsyłania spamu w Internecie. Listy te są wykorzystywane przez administratorów pocztowych do blokowania znanych serwerów rozsyłających spam.

Jak sprawdzić, czy serwer znajduje się na liście RBL

Jeżeli znajdziesz swój serwer na jakiejś liście RBL, istnieją duże szanse, że jest uruchomiony w trybie "open relay", chyba, że ostatnio modyfikowałeś jego konfigurację. Mogło się też zdarzyć, że któryś z Twoich legalnych użytkowników nadużył serwer i rozsyłał spam bądź jakieś "komunikaty". Takie przypadki też często są przyczyną umieszczenia serwera na liście. Aby sprawdzić czy serwer znajduje się na jakiejś liście zajrzyj na:

<http://www.mail-abuse.com/support/lookup.html>

<http://www.ordb.org/>

Pamiętaj, że istnieje wiele list RBL, a na powyższych stronach znajdują się tylko te najlepiej znane.

* Audyt serwera pocztowego

Audyt serwera pocztowego pozwala na identyfikację słabych punktów, które mogą zostać złośliwie wykorzystane do wykonania operacji na lub za pośrednictwem serwera pocztowego.

Nessus

Nessus jest darmowym zdalnym skanerem podatności, który zawiera także pluginy poświęcone testom bezpieczeństwa MTA. Umożliwia szybką i efektywną weryfikację luk w serwerach SMTP.

Nessus oraz pluginy do niego dostępne są na stronie www.nessus.org.

SARA

Sara (Security Auditor's Research Assistant) to skaner podatności, który uwzględnia także podatności na liście SANS Top 20.

SARA dostępna jest na stronie <http://www-arc.com/sara/>

U5.5 Jak się przed tym chronić?

Aby zabezpieczyć swój serwer pocztowy, należy podjąć następujące dwa kroki. Pierwszy krok dotyczy zaleceń niezależnych od konkretnej implementacji serwera pocztowego, drugi krok poświęcony jest konkretnej implementacji, takim jak Sendmail, Qmail oraz Postfix.

1. Ogólne zalecenia

- należy zdecydować czy naprawdę konieczne jest uruchomienie serwera MTA i czy powinien być dostępny z poziomu Internetu
- wyłączyć MTA na serwerach, które nie zostały wyznaczone do pełnienia tej funkcji. Należy opracować procedury, które by zapobiegały przypadkowemu uruchomieniu.

Warto w tym celu wykorzystać firewalle do zablokowania możliwości połączeń przychodzących i wychodzących.

- Należy zainstalować najnowsze łaty lub uaktualnić system do najnowszej wersji
- Należy wydzielić wewnętrzny MTA do obsługi poczty wewnętrznej
- Należy ograniczyć przywileje procesu pod którym uruchomiony jest serwer MTA bądź uruchamiać serwer w środowisko "chroot".
- Należy zapoznać się z dokumentacją serwera i zapisać się na odpowiednie listy dyskusyjne

Ochrona przed nieupoważnionym przekazywaniem poczty (mail relaying)

W celu uniknięcia wykorzystania serwera przez spamatorów, serwer powinien być skonfigurowany tak aby nie służył jako relay dla nieupoważnionych sieci i domen.

Sendmail

Jeżeli musisz uruchamiać Sendmaila jako demon, upewnij się, że konfiguracja pozwala na relay'owanie poczty tylko dla systemów pod Twoim nadzorem. Zobacz

<http://www.sendmail.org/tips/relaying.html> i

http://www.sendmail.org/m4/anti_spam.html - pomoc w zakresie poprawnej konfiguracji serwera. Poczynając od Sendmail 8.9.0, otwarte relay'owanie zostało domyślnie wyłączone. Jednakże wielu producentów systemów ponownie włączyło tę możliwość. Jeżeli wykorzystywany jest Sendmail, który był dostarczony wraz z systemem, należy upewnić się, że nie może być wykorzystany w charakterze relay.

Qmail

Qmail oferuje solidną dokumentację na temat selektywnego relay'owania i o tym jak wyłączyć relay'owanie na swoim systemie. Patrz:

<http://www.lifewithqmail.org/lwq.html#relaying>

Courier-MTA

Courier dostarcza informacji jak otwierać relay dla wybranych sieci i IP. Courier pozwala na relay za pomocą SMTP Authentication.

<http://www.courier-mta.org> - sekcja FAQ

Exim

Exim także posiada dokładne instrukcje jak zabezpieczać się przed relay'owaniem:

<http://www.exim.org/howto/relay.html>

Postfix

W przypadku Postfix'a istnieje szereg kroków jakie można podjąć w celu ograniczenia relay'owania i kontroli dostępu. Tylko hosty i sieci wpisane do parametru 'mynetworks' będą upoważnione do przekazywania poczty:

http://www.postfix.org/SMTPD_ACCESS_README.html

2. Zalecenia dotyczące konkretnych implementacji

A) Dodatkowe informacje o tym jak konfigurować i uruchamiać Sendmaila w sposób bezpieczny są dostępne na stronach:

<http://www.sendmail.org/secure-install.html>

http://www.sendmail.org/m4/security_notes.html

<http://www.sendmail.org/~gshapiro/security.pdf>

B) W celu ograniczenia ewentualnego włamania do Postfixa, należy serwer Postfixa uruchomić z prawami użytkownika nieuprzywilejowanego w środowisku "chroot":

<http://www.linuxjournal.com/article.php?sid=4241>

C) Poniższy link zawiera przykłady jak skonfigurować MTA tak aby korzystać z "blackholing":

<http://www.ordb.org/faq/#usage>

D) Courier-MTA domyślnie wspiera listy RBL, i dostarcza taką listę w pliku konfiguracyjnym esmtpd

E) Postfix wspiera wiele możliwości ograniczenia spamu, informacje na ten temat można znaleźć na następującej stronie:

<http://www.securitysage.com/antispam/intro.html>

[przejdź do początku dokumentu ^](#)

U6 Simple Network Management Protocol (SNMP)

U6.1 Opis

Simple Network Management Protocol (SNMP) jest protokołem szeroko wykorzystywanym do zdalnego monitorowania i konfiguracji prawie wszystkich nowoczesnych urządzeń TCP/IP. Chociaż SMTP spotykany jest na bardzo różnych platformach, najczęściej wykorzystuje się go do konfiguracji i zarządzania takich urządzeń jak drukarki, routery, switchy i access pointy, oraz w celu dostarczania informacji sieciowym systemom monitorowania.

Komunikacja SNMP opiera się na różnych rodzajach komunikatów wymienianych pomiędzy stacjami zarządzającymi a urządzeniami sieciowymi, na których umieszczone jest oprogramowanie zwane agentem. Sposób, w jaki te komunikaty są przetwarzane, oraz mechanizm uwierzytelniający jest bardzo podatny na różne ataki.

Luki w metodzie, w jakiej SNMP w wersji 1 przetwarza komunikaty i generuje trapy, są opisane szczegółowo w CERT Advisory CA-2002-03. Istnieje szereg luk w sposobie, w jaki trapy i zapytania są przetwarzane i dekodowane, zarówno na stacjach zarządzających jak i agentach. Luki te, bez względu na producenta, nie dotyczą tylko konkretnych implementacji SNMP, ale ich całego szeregu. Skutkiem wykorzystania tych luk może być Denial of Service bądź niepożądana konfiguracja i nieupoważnione zarządzanie urządzeniami posiadającymi wsparcie dla SNMP.

W starszych architekturach SNMP wbudowany mechanizm uwierzytelnienia także stanowi poważne zagrożenie. SNMP w wersji 1 i 2 korzysta z nieszyfrowanego „community string” jako jedynego mechanizmu uwierzytelniającego. Brak szyfrowania jest poważną wadą, ale jeszcze poważniejszą jest fakt, że „community string” jest domyślnie ustawione w większości urządzeń na „public”. Część producentów zmienia „community string” na „private” dla bardziej wrażliwych informacji. Atakujący może tę wiedzę wykorzystać do zdalnej rekonfiguracji bądź wyłączenia urządzenia. Podłuchany ruch SNMP może wyjawiać wiele informacji na temat struktury sieci oraz podłączonych do niej systemów i urządzeń. Włamywacze wykorzystują tego typu informacje do wyboru celów i planowania ataków.

Większość producentów domyślnie uruchamia SNMP w wersji 1 na swoich urządzeniach, a wielu nie korzysta z mechanizmów bezpieczeństwa oferowanych przez SNMP wersja 3, które można skonfigurować tak, aby skorzystały z lepszych metod uwierzytelnienia. Jednakże istnieją też darmowe implementacje SNMPv3, rozpowszechniane na licencji GPL lub BSD.

SNMP nie jest spotykane tylko na systemach UNIX, jest szeroko wykorzystywane na systemach Windows, w sprzęcie sieciowym, w bezprzewodowych punktach dostępu, drukarkach i *embedded devices*. Jednak większość ataków zaobserwowanych do tej pory dotyczy systemów UNIX, ze słabymi konfiguracjami SNMP. Należy pamiętać, że SNMP jest transmitowane otwartym tekstem, więc sytuacje, w których takich ruch może zostać podsłuchany powinny być brane pod uwagę.

CERT/CC opublikował dokument na temat luk związanych z SNMP:

http://www.cert.org/tech_tips/snmp_faq.html

U6.2 Podatne systemy operacyjne

Prawie wszystkie dystrybucje UNIX i Linux mają, a często też domyślnie uruchamiane SNMP. Większość innych urządzeń sieciowych SNMP i systemów operacyjnych jest również podatnych na atak.

U6.3 Wpisy CVE/CAN

[CVE-1999-0294](#) [CVE-1999-0472](#) [CVE-1999-0815](#) [CVE-1999-1335](#) [CVE-2000-0221](#)
[CVE-2000-0379](#) [CVE-2000-0515](#) [CVE-2000-1058](#) [CVE-2001-0236](#) [CVE-2001-0487](#)
[CVE-2001-0514](#) [CVE-2001-0564](#) [CVE-2001-0888](#) [CVE-2002-0017](#) [CVE-2002-0069](#)
[CVE-2002-0302](#) [CAN-1999-0186](#) [CAN-1999-0254](#) [CAN-1999-0499](#) [CAN-1999-0516](#)
[CAN-1999-0517](#) [CAN-1999-0615](#) [CAN-1999-0792](#) [CAN-1999-1042](#) [CAN-1999-1126](#)
[CAN-1999-1245](#) [CAN-1999-1460](#) [CAN-1999-1513](#) [CAN-2000-0147](#) [CAN-2000-0885](#)
[CAN-2000-0955](#) [CAN-2000-1157](#) [CAN-2000-1192](#) [CAN-2001-0046](#) [CAN-2001-0352](#)
[CAN-2001-0380](#) [CAN-2001-0470](#) [CAN-2001-0552](#) [CAN-2001-0566](#) [CAN-2001-0711](#)
[CAN-2001-0840](#) [CAN-2001-1210](#) [CAN-2001-1220](#) [CAN-2001-1221](#) [CAN-2001-1262](#)
[CAN-2002-0012](#) [CAN-2002-0013](#) [CAN-2002-0053](#) [CAN-2002-0109](#) [CAN-2002-0305](#)
[CAN-2002-0478](#) [CAN-2002-0540](#) [CAN-2002-0812](#) [CAN-2002-1048](#) [CAN-2002-1170](#)
[CAN-2002-1408](#) [CAN-2002-1426](#) [CAN-2002-1448](#) [CAN-2002-1555](#) [CAN-2003-0137](#)
[CAN-2003-0935](#) [CAN-2003-1002](#) [CAN-2004-0311](#) [CAN-2004-0312](#) [CAN-2004-0576](#)
[CAN-2004-0616](#) [CAN-2004-0635](#) [CAN-2004-0714](#)

U6.4 Jak sprawdzić czy Twój system jest podatny na atak?

Fakt czy SNMP jest uruchomione na sieciowych urządzeniach można zweryfikować za pomocą skanerów lub ręcznie.

- SNMPing – Darmowe narzędzie do skanujowania. Można je uzyskać z SANS Institute ze strony: <http://www.sans.org/alerts/snmp/>
- SNScan – Firma Foundstone stworzyła łatwe do użycia narzędzie skanujące SNMP, znane jako SNScan, dostępne na stronie: http://www.foundstone.com/knowledge/free_tools.html.
- Nessus – skaner podatności (narzędzie jest open source) – <http://www.nessus.org>

Jeżeli nie można wykorzystać jednego z wyżej wymienionych narzędzi, trzeba ręcznie zweryfikować fakt działania SNMP. W tym celu należy zapoznać się z dokumentacją systemu operacyjnego. Jednak podstawowy demon może być zazwyczaj zidentyfikowany przez grepa na ciąg „snmp” w liście procesów bądź przez sprawdzenie, czy na portach 161 lub 162 rezydują jakieś usługi (narzędzie lsof jest przydatne w mapowaniu portów na procesy, które je wykorzystują).

Uruchomiona instancja SNMP jest prawdopodobnie wystarczającym dowodem na to, że system jest podatny na błędy w przetwarzaniu trapów i zapytań. Więcej informacji na ten temat można przeczytać w zaleceniu CERT Advisory CA-2002-03.

Jeżeli SNMP jest uruchomiony, możliwe jest, że konfiguracja zawiera następujące błędy:

1. Puste lub domyślne SNMP „community names”.
2. Łatwe do odgadnięcia SNMP „community names”.
3. Ukryte SNMP „community strings”.

Więcej informacji, jak zidentyfikować powyższy stan rzeczy dostępnych jest na stronie: <http://www.sans.org/resources/idfaq/snmp.php>

U6.5 Jak się przed tym chronić?

Luki w przetwarzaniu zapytań i trapów:

1. Jeżeli nie potrzebujesz SNMP, wyłącz go.
2. W miarę możliwości, należy wykorzystać model bezpieczeństwa SNMPv3, z uwierzytelnieniem komunikatów i szyfrowaniem zawartości.
3. Jeżeli korzystanie z SNMPv1 lub v2 jest konieczne, należy upewnić się, że jest to wersja załatana przez producenta. Dobrym punktem startowym do uzyskania informacji na temat implementacji konkretnych producentów jest Appendix A zalecenia CERT Advisory CA-2003-03.
4. Należy filtrować SNMP (port 161 TCP/UDP i 162 TCP/UDP) na punktach wejściowych do Twoich sieci, chyba że absolutnie niezbędne jest odpytywanie i zarządzanie urządzeniami z zewnątrz.
5. Należy skonfigurować kontrolę dostępu na podstawie hostów na systemach z agentami SNMP. Chociaż ta możliwość może być bardzo ograniczona w zależności od systemu operacyjnego, na którym jest agent SNMP, kontrola z jakich systemów agent przyjmuje zapytania może być możliwa. Na większości systemów UNIX odbywa się to poprzez pakiet TCP-Wrappers bądź odpowiednią konfiguracją Xinetd. Firewall na systemie z agentem może także być wykorzystany do blokowania niepożądanych zapytań SNMP.

Domyślne i łatwe do odgadnięcia „community names”:

1. Jeżeli nie potrzebujesz SNMP, wyłącz go.
2. W miarę możliwości, należy wykorzystać model bezpieczeństwa SNMPv3, z uwierzytelnieniem komunikatów i szyfrowaniem zawartości.
3. Jeżeli korzystanie z SNMPv1 lub v2 jest konieczne, ta sama polityka zarządzania hasłami, jaka jest stosowana do zwykłych haseł, powinna zostać zastosowana w stosunku do community names. Hasła muszą być trudne do odgadnięcia lub złamania i regularnie zmieniane.
4. Zweryfikuj i sprawdź „community names” za pomocą „snmpwalk”. Dodatkowe informacje można odszukać na stronie: <http://www.zend.com/manual/function.snmpwalk.php>. Dobry tutorial na temat tego narzędzia znajduje się pod adresem: <http://www.sans.org/resources/idfaq/snmp.php>.
5. Należy filtrować SNMP (port 161 TCP/UDP i 162 TCP/UP) na punktach wejściowych do Twoich sieci, chyba że absolutnie niezbędne jest odpytywanie i zarządzanie urządzeniami z zewnątrz. Wtedy, jeżeli to możliwe, skonfiguruj filtry tak, aby ruch SNMP był wpuszczany tylko z zaufanych podsieci.

Kiedy tylko możliwe, bazy MIB powinny być dostępne tylko do odczytu. Więcej informacji na ten temat jest na stronie:
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315.

[przejdź do początku dokumentu ^](#)

U7 Open Secure Sockets Layer (SSL)

U7.1 Opis

Open source'owa biblioteka [OpenSSL](#) jest popularnym pakietem wzbogacającym aplikacje komunikujące się przez sieć o kryptograficzne mechanizmy bezpieczeństwa. Jest szeroko wykorzystwaną implementacją SSL/TLS, stosowaną przez wielu producentów. Najbardziej znaną aplikacją korzystającą z tej biblioteki jest serwer WWW Apache (do bezpiecznych połączeń http). Serwery POP, IMAP, SMTP i LDAP także mają swoje OpenSSL'owe odpowiedniki.

Zazwyczaj OpenSSL jest wykorzystywany jako zestaw narzędzi, które inne aplikacje wykorzystują do zapewnienia kryptograficznej ochrony dla połączeń sieciowych. Zamiast atakowania OpenSSL bezpośrednio, exploity są skierowane na aplikacje wykorzystujące OpenSSL. Kilka znany exploit'ów atakuje serwery Apache korzystające z OpenSSL. Tak więc fakt, że korzystasz z serwera Apache z OpenSSL nie znaczy, że jesteś bezpieczny. Odpowiednio zmodyfikowany exploit może zostać wykorzystany do zaatakowania Sendmail, openldap, CUPS lub innego programu wykorzystującego OpenSSL.

Znaleziono wiele luk w OpenSSL, z których najbardziej poważne to pięć opisanych w [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0557](#), [CAN-2002-0659](#) oraz [CAN-2003-0545](#). Umożliwiają one zdalne wykonanie dowolnego kodu z przywilejami użytkownika korzystającego z bibliotek OpenSSL (w niektórych przypadkach, takich jak 'sendmail', jest to root).

U7.2 Podatne systemy operacyjne

Każdy system UNIX i Linux z OpenSSL 0.9.7 lub wcześniejszymi wersjami. Należy zwrócić uwagę, że OpenSSL jest często instalowane jako wsparcie dla innego komponentu. Na przykład na systemie RedHat Linux 9.0 pakiety takie jak Apache, CUPS, Curl, OpenLDAP, Stunnel i Sendmail (między innymi) wykorzystują biblioteki OpenSSL do zabezpieczania połączeń.

U7.3 Wpisy CVE/CAN

[CVE-1999-0428](#), [CVE-2001-1141](#)

[CAN-2000-0535](#), [CAN-2002-0655](#), [CAN-2002-0656](#), [CAN-2002-0557](#), [CAN-2002-0659](#), [CAN-2003-0078](#), [CAN-2003-0131](#), [CAN-2003-0147](#), [CAN-2003-0543](#), [CAN-2003-0544](#), [CAN-2003-0545](#), [CAN-2003-0851](#), [CAN-2004-0079](#), [CAN-2004-0081](#), [CAN-2004-0112](#), [CAN-2004-0607](#)

U7.4 Jak sprawdzić czy Twój system jest podatny na atak?

Sprawdź, co wyświetla polecenie 'openssl version'. Jeżeli nie jest to wersja 0.9.7d lub 0.9.6m, jesteś podatny na atak.

U7.5 Jak się przed tym chronić?

1. Zaktualizuj bibliotekę [OpenSSL](#) do najnowszej wersji. Jeżeli OpenSSL otrzymałeś wraz z systemem operacyjnym, ściągnij najnowsze łaty od producenta systemu. W niektórych przypadkach konieczne będzie rekompilowanie i/lub ponowne linkowanie aplikacji, aby korzystały z nowych bibliotek.
2. Jeżeli jest to możliwe w Twoim środowisku, aby ograniczyć dostęp do serwera OpenSSL, rozważ wykorzystanie pakietu ipfilter bądź innych narzędzi do filtrowania pakietów. Należy pamiętać jednak, że najczęściej OpenSSL jest wykorzystywane do zabezpieczania ruchu HTTP przekazywanego przez Internet na potrzeby e-commerce, więc takie posunięcie może być niemożliwe.

[przejdź do początku dokumentu](#) ^

U8 Błędy w konfiguracji NIS/NFS

U8.1 Opis

Network File System (NFS) i Network Information Services (NIS) to dwie ważne usługi wykorzystywane w sieciowych systemach UNIX. NFS to usługa stworzona przez Sun Microsystems, w celu udostępniania plików przez sieć systemom UNIX. NIS to zestaw usług, tworzących bazę danych (składającą się z tzw. map), świadcząca usługi informacyjne innym usługom sieciowym, jak np.: Network File System NFS. Najczęściej mapy to pliki passwd i group, wykorzystywane w charakterze centralnego systemu uwierzytelnienia użytkowników.

Problemy bezpieczeństwa obydwu usług stale się pojawiają (przepełnienie bufora, DoS, słabe uwierzytelnienie) i sprawiają, że usługi te są częstym przedmiotem ataków.

Poza wieloma często spotykanymi przypadkami niezalotanych usług, duże zagrożenie stanowi słaba konfiguracja NFS i NIS, pozwalająca na wykorzystanie luk przez zdalnych i lokalnych użytkowników.

Słabe uwierzytelnienie w systemie NIS podczas wysyłania zapytań do map NIS można wykorzystać za pomocą aplikacji takich jak ypcat lub getent, która wyświetla wartości map, i uzyskać plik z hasłami. Podobny problem jest z NFS, które opiera się na zaufaniu do identyfikatora użytkownika (UID) oraz grupy (GID), przedstawianych serwerowi przez klienta NFS. W zależności od konfiguracji serwera może to pozwolić dowolnemu użytkownikowi podmontowanie i podgląd zdalnego systemu plików.

U8.2 Podatne systemy operacyjne

Prawie wszystkie systemy UNIX i Linux są dystrybuowane z zainstalowanym NFS i NIS - często domyślnie uruchamianych. W przypadku NFS, domyślnie pliki "exports" (pliki te specyfikują katalogi, które mają być współdzielone) są zazwyczaj puste.

U8.3 Wpisy CVE/CAN

NFS

[CVE-1999-0002](#), [CVE-1999-0166](#), [CVE-1999-0167](#), [CVE-1999-0170](#), [CVE-1999-0211](#), [CVE-1999-0832](#), [CVE-1999-1021](#), [CVE-2000-0344](#), [CVE-2002-0830](#)

[CAN-1999-0165](#), [CAN-1999-0169](#), [CAN-2000-0800](#), [CAN-2002-0830](#), [CAN-2002-1228](#), [CAN-2003-0252](#), [CAN-2003-0379](#), [CAN-2003-0576](#), [CAN-2003-0680](#), [CAN-2003-0683](#), [CAN-2003-0976](#), [CAN-2004-0154](#)

NIS

[CVE-1999-0008](#), [CVE-1999-0208](#), [CVE-1999-0245](#), [CVE-2000-1040](#)

[CAN-1999-0795](#), [CAN-2002-1232](#), [CAN-2003-0176](#), [CAN-2003-0251](#)

U8.4 Jak sprawdzić czy Twój system jest podatny na atak?

Niezbędne jest podjęcie następujących kroków, mających na celu sprawdzenie, czy oprogramowanie NIS/NFS nie posiada luk:

1. Należy sprawdzić czy wersje są aktualne pod kątem łat wypuszczonych przez producenta. W większości przypadków, polecenie `rpc.mountd -version` dla NFS i `ypserv -version` dla NIS podaje wersje usług. Każda niezafatana lub przestarzała wersja oprogramowania jest prawdopodobnie podatna na atak.
2. Aby zweryfikować potencjalne luki, wskazane jest skorzystanie z aktualnego skanera podatności, i regularne sprawdzanie czy system posiada błędy bezpieczeństwa.
3. Jeżeli możliwe, wykorzystaj Blowfish lub MD5 zamiast DES dla skrótów haseł.

Następujące kroki mają na celu stwierdzenie jakości konfiguracji NIS:

1. Zadbaj o to, żeby hasło roota nie było trzymane w mapie NIS.
2. Sprawdź, czy hasła użytkowników są odpowiednio silne. W tym celu można wykorzystać narzędzie do łamania haseł.

Uwaga: Nigdy nie uruchamiaj narzędzia do łamania haseł, nawet na systemach, na których masz uprawnienia root, bez wyraźnej, najlepiej pisemnej zgody kierownictwa lub pracodawcy. Zdarzało się, że administratorów, którzy mieli jak najlepsze intencje, zwalniano za działanie bez pozwolenia. Pozwolenie to powinno być w postaci listu i tworzyć część polityki zarządzania hasłami organizacji, która zezwala na okresowe sprawdzanie jakości haseł.

Następujące kroki mają na celu stwierdzenie jakości konfiguracji NFS:

1. Należy zweryfikować, czy hosty, netgroupy i prawa w pliku `/etc/exports` są aktualne.
2. Aby zobaczyć, co jest eksportowane, uruchom polecenie `showmount -e IP_SERWERA`. Sprawdź czy to, co montujesz lub eksportujesz jest zgodne z Twoją polityką bezpieczeństwa.

U8.5 Jak się przed tym chronić?

Poniższe kroki dotyczą konfiguracji NIS:

1. Każdy klient powinien posiadać listę serwerów NIS, do których może się połączyć. Pomaga to zapobiec podszyciu się pod serwer NIS.
2. Podczas tworzenia plików DBM, uruchom opcję `YP_SECURE`, aby upewnić się, że serwer NIS będzie odpowiadał na zapytania klienta pochodzące z portów uprzywilejowanych. Opcję tę można włączyć, stosując flagę `s` z poleceniem `makedbm`.
3. Dodaj zaufane hosty i sieci do pliku `/var/yp/securenets`, wykorzystywanego przez procesy `ypserv` i `ypxfrd`, i pamiętaj zrestartować demony aby zmiany miały natychmiastowy efekt.
4. Upewnij się, że klienci NFS posiadają wpis `+:*:0:0:::` w mapie haseł.

5. Rozważ wykorzystanie bezpiecznego protokołu SSH w NIS. Dobrym punktem startowym jest dokument dostępny na stronie:
<http://www.math.ualberta.ca/imaging/snfs/>.

Uwaga: Protokół LDAP (Lightweight Directory Access Protocol) jest w stanie zastąpić NIS w wielu przypadkach. Wszystkie dystrybucje Linuxa wspierają LDAP jako centralne źródło przechowujące dane dotyczące haseł, grup i hostów. Warto zapoznać się z dobrą książką dotyczącą administracji LDAP. LDAP domyślnie wspiera SSL i replikacje.

Poniższe kroki dotyczą konfiguracji NFS:

1. Korzystaj z numerycznych adresów IP lub nazw kanonicznych (FQDN) zamiast aliasów, kiedy wpisujesz klientów do `/etc/exports`.
2. Wykorzystaj plik `/etc/exports` do ograniczenia dostępu do systemu plików NFS:
 - o Zablokuj możliwość montowania systemu plików NFS zwykłym użytkownikom poprzez dodanie parametru `secure` po adresie IP bądź nazwie klienta NFS (na przykład: `/home 10.20.1.25(secure)`).
 - o Eksportuj system plików NFS tylko z odpowiednimi prawami. Można to zrobić poprzez dodanie opcji specyfikujących prawa (`ro` dla tylko do odczytu lub `rw` dla pisania i czytania) po adresie IP bądź nazwie klienta NFS w pliku `/etc/exports` (na przykład: `/home 10.20.1.25(ro)`).
 - o Jeżeli to możliwe, wykorzystaj parametr `root_squash` po adresie IP bądź nazwie klienta NFS. Jeżeli ten parametr jest włączony, superużytkownik z prawami roota na kliencie NFS zostanie zastąpiony użytkownikiem `nobody` lub grupy `nobody` (w zależności od parametrów `anonuid` i `anongid`) na serwerze NFS. Oznacza to, że root na kliencie nie może mieć dostępu lub modyfikować plików, do których tylko root na serwerze może mieć dostęp lub prawo modyfikacji (np.: `/home 10.20.1.25(root_squash)`).
 - o Jeżeli chcesz eksportować katalog dla anonimowych użytkowników, wykorzystaj parametr `"all_squash"`, który mapuje każdy `userid` i każdą grupę do ID ustalonego przez `anonuid` i `anongid`.
 - o Pełny wykaz parametrów znajduje się w instrukcji `man /etc/exports` lub na sieci <http://www.netadmintools.com/html/5exports.man.html>
3. Jeżeli Twój system to Solaris, upewnij się, że masz włączoną opcję `Port Monitoring`. Opcję tę aktywuje się poprzez dodanie linijki `set nfssrv:nfs_portmon = 1` w pliku `/etc/system`. Systemy Linux domyślnie nie zezwalają na współpracę z klientami NFS wykorzystującymi niezarezerwowany port.
4. Narzędzie `NFSBug` może być wykorzystane do testowania konfiguracji. Testy sprawdzają czy systemy plików są eksportowane na świat, czy ograniczenia na eksportowane systemy plików działają, czy systemy plików mogą być montowane za pośrednictwem `portmappera`. Próbuje odgadnąć handle plików i sprawdzają wiele błędów umożliwiających dostęp do systemów plików.
<http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/nfsbug/>

Ogólne punkty do rozważenia dotyczące NIS i NFS:

1. Przejrzyj swoją politykę firewallowania, i zablokuj wszystkie niepotrzebne porty, w szczególności port `111/tcp/udp` (`portmap`) i port `2049/tcp/udp` (`rpc.nfsd`). Pozwalaj na dostęp do serwerów NIS i NFS tylko od upoważnionych klientów. Filtrowanie można też dokonać na poziomie serwera za pomocą `tcp_wrappers`,

- <http://sunsite.cnlab-switch.ch/ftp/software/security/security-porcupine.org/>. W pliku /etc/hosts.allow wpisz usługę oraz IP upoważnione do dostępu do serwisu (np.: portmap: 10.20.0.0/16, aby pozwolić na dostęp z sieci 10.20.0.0 do usługi portmap). Także w pliku /etc/hosts.deny należy dodać usługi i IP które nie mogą mieć dostępu do serwisów (np.: portmap: ALL, co zablokuje dostęp ze wszystkich IP nie zawartych w /etc/hosts.allow). Portmap jest ważną usługą, która powinna być zablokowana. Jest bowiem jedną z tych, które wykorzystuje NFS.
2. Rozważ wykorzystanie NFS za pośrednictwem bezpiecznego protokołu, takim jak SSH. Dobrym punktem startowym jest: <http://www.math.ualberta.ca/imaging/snfs/>.
 3. Stosuj wszystkie łaty producentów bądź zaktualizuj swoje serwery NIS i NFS do najnowszej wersji. Więcej informacji na temat zabezpieczania instalacji UNIX dostępnych jest na stronie CERT-u, [UNIX Security Checklist](#).

Wyłącz demony NFS i NIS na wszystkich systemach, które nie zostały wyznaczone do pełnienia tej roli. Aby uniemożliwić ponowne uruchomienie usługi, rozsądnym krokiem może być całkowite odinstalowanie oprogramowania NFS i/lub NIS.

[przejdź do początku dokumentu ^](#)

U9 Bazy danych

U9.1 Opis

Bazy danych stanowią element biznesu elektronicznego, finansów, bankowości, i systemów ERP (Enterprise Resource Planning) i zawierają krytyczne informacje od partnerów, klientów oraz pracowników. Chociaż waga utrzymania integralności danych oraz ich poufności jest znana, w systemach DBMS (database management systems) w przeszłości często nie stosowano zabezpieczeń tak jak na poziomie systemów operacyjnych i sieci. Systemy DBMS to programy, które odpowiedzialne są za przechowywanie, modyfikacje i ekstrakcje danych z baz danych.

Integralność i poufność danych może zależeć od wielu czynników, takich jak stopień skomplikowania danej implementacji, słabości haseł, błędów w konfiguracji, słabo napisanego kodu aplikacji, stałych haseł, oraz nierozpoznanych tylnych furtek. Większość przedsiębiorstw oraz organizacji rządowych wykorzystuje bazy danych do przechowywania danych osobowych, takich jak listy płac i dokumentacje medyczną, co do których są ustawowo zobowiązani do zapewnienia integralności i poufności. Bazy danych zawierają wrażliwe dane finansowe, w tym informacje o transakcjach biznesowych i dane księgowe. Przechowują także dokładne dane o klientach, takie jak informacje o stanie kont, numery kart kredytowych i wrażliwe dane partnerów biznesowych.

Bazy danych to niezwykle skomplikowane aplikacje, i często jest je trudno odpowiednio skonfigurować i zabezpieczyć. Bazy danych takie jak MYSQL, Postgres i ORACLE posiadają wiele wrażliwych cech: konta i hasła użytkowników, systemy audytowe, przywileje i prawa dostępu do obiektów baz danych, wbudowane polecenia, unikalne języki skryptowe i języki programowania, protokoły sieciowe, łaty, rozbudowane systemy zarządzające itp. Wielu administratorów zajmuje się bazami danych z przypadku i tylko od czasu do czasu, i często nie rozumie tego stopnia skomplikowania. W efekcie poważne błędy w zabezpieczeniach i konfiguracji pozostają niezauważone. Środowisko zajmujące się bezpieczeństwem z reguły ignorowało temat bezpieczeństwa baz danych. Z kolei wielu specjalistów od baz danych nie uważało kwestii bezpieczeństwa za ich odpowiedzialność. Większość baz danych posiada wiele

cech i możliwości, które mogą zostać wykorzystane do naruszenia integralności, poufności i dostępności danych które przechowują.

Wszystkie nowoczesne relacyjne bazy posiadają możliwość bezpośredniego ich odpytywania za pomocą specjalnych narzędzi, z pominięciem tradycyjnych zabezpieczeń na poziomie systemu operacyjnego. Na przykład dostęp do baz danych ORACLE można uzyskać za pośrednictwem portu 1521/tcp, MySQL z kolei za pośrednictwem 3306/tcp, a Postgres portu 5432/tcp. Większość aplikacji baz danych posiada dobrze znane domyślne konta i hasła, które mogą posłużyć do uzyskania dostępu do danych na różnych poziomach. Obecnie większość baz jest mocno powiązana z aplikacjami typu front-end, w większości aplikacjami WWW. Jeżeli aplikacja jest słabo napisana lub skonfigurowana, atakujący może przeprowadzić atak „SQL injection” lub wykorzystać luki w bazie danych.

CERT/CC opublikował zalecenie, [CA-2003-05](#), na wiele luk w ORACLE, które mogą być wykorzystane do włamania się do bazy danych. Ostatnio, US-CERT wydał zalecenie na temat SQL Injection Vulnerabilities in Oracle E-Business Suite ([TA04-160A](#)), które może doprowadzić do naruszenia integralności bazy danych.

MySQL również posiada kilka znanych luk. Ogólny opis kilku ataków można znaleźć w ostatnich opublikowanym dokumencie Next Generation Software, <http://www.nextgenss.com/papers/HackproofingMySQL.pdf>

U9.2 Podatne systemy operacyjne

Prawie wszystkie dystrybucje Linuxa zawierają oprogramowanie open source DBMS, takie jak MySQL lub PostgreSQL, lub komercyjne oprogramowanie ORACLE. Wiele wariantów systemu Unix, takie jak Solaris, AIX, HPUX, wspiera ORACLE, DB2 i inne komercyjne DBMS, a także wymienione już wcześniej oprogramowanie open source DBMS.

U9.3 Wpisy CVE/CAN

Oracle:

[CVE-2002-0567](#), [CVE-2002-0571](#)

[CAN-1999-0652](#), [CAN-1999-1256](#), [CAN-2002-0858](#), [CAN-2002-1264](#), [CAN-2003-0095](#), [CAN-2003-0096](#), [CAN-2003-0222](#), [CAN-2003-0634](#), [CAN-2003-0727](#), [CAN-2003-0894](#)

MySQL:

[CVE-1999-1188](#), [CVE-2000-0045](#), [CVE-2000-0148](#), [CVE-2000-0981](#), [CVE-2001-0407](#)

[CAN-1999-0652](#), [CAN-2001-1274](#), [CAN-2001-1275](#), [CAN-2002-0229](#), [CAN-2002-0969](#), [CAN-2002-1373](#), [CAN-2002-1374](#), [CAN-2002-1375](#), [CAN-2002-1376](#), [CAN-2003-0073](#), [CAN-2003-0150](#), [CAN-2003-0515](#), [CAN-2003-0780](#), [CAN-2004-0381](#), [CAN-2004-0388](#), [CAN-2004-0627](#), [CAN-2004-0628](#)

PostgreSQL:

[CVE-2002-0802](#)

[CAN-1999-0862](#), [CAN-2000-1199](#), [CAN-2001-1379](#), [CAN-2002-0972](#), [CAN-2002-1397](#), [CAN-2002-1398](#), [CAN-2002-1399](#), [CAN-2002-1400](#), [CAN-2002-1401](#), [CAN-2002-1402](#), [CAN-2003-0040](#), [CAN-2003-0500](#), [CAN-2003-0515](#), [CAN-2003-0901](#), [CAN-2004-0366](#), [CAN-2004-0547](#)

U9.4 Jak sprawdzić czy Twój system jest podatny na atak?

Należy się upewnić, że wszelkie uruchomione oprogramowanie DBMS to najbardziej aktualne wersje. Niezałatane, bądź stare wersje są prawdopodobnie podatne na atak.

Domyślne instalacje DBMS są najprawdopodobniej podatne na atak.

Należy przeskanować zainstalowane aplikacje pod kątem podatności:

- **MySQL Network Scanner**: umożliwia przeskanowanie sieci pod kątem instalacji MySQL z pustymi hasłami i może posłużyć także do zidentyfikowania niepotrzebnych instancji serwerów MySQL.
- **Nessus** (<http://www.nessus.org>), darmowy skaner podatności, rozpoznaje częste luki w bazach na systemach Unix.
- Komercyjne skanery podatności, takie jak Foundstone, Qualys czy eEye Retina, także mogą być wykorzystane do wykrycia luk w bazach danych
- Istnieją także skanery dedykowane dla baz danych, takie jak: AppSecInc lub ISS Database Scanner

U9.5 Jak się przed tym chronić?

Konieczne jest potwierdzenie, że aplikacje baz danych są odpowiednio załatane.

Sprawdź stronę odpowiedniego producenta:

- **Oracle** (<http://otn.oracle.com/software/index.html>)
- **MySQL** (<http://www.mysql.com/products/mysql/>)
- **PostgreSQL** (<ftp://ftp.postgresql.org/pub>)

Następnie upewnij się, że DBMS i aplikacje zostały odpowiednio zabezpieczone:

- Stosuj zasadę najmniejszych przywilejów.
- Usuń lub zmień domyślne hasła na bazie przed wykorzystaniem uruchomieniem systemu w sieci.
- Wykorzystaj mechanizm stored procedure kiedy to możliwe.
- Usuń/wyłącz niepotrzebne mechanizmy stored procedure.
- Ustal limity długości na formularzach.
- Waliduj wszystkie dane po stronie serwera (długość, format, typ).

Istnieje szereg dokumentów dotyczących bezpieczeństwa DBMS:

- **Oracle** (<http://otn.oracle.com/deploy/security/index.html>)
- **MySQL** (<http://dev.mysql.com/doc/mysql/en/Security.html>)
- **PostgreSQL** (<http://www.postgresql.org/docs/7/interactive/security.htm>)

Warto być na bieżąco z podatnościami i alertami ogłaszanymi przez producentów:

- **Oracle Security Alerts** (<http://otn.oracle.com/deploy/security/alerts.htm>)
- **MySQL** (<http://lists.mysql.com/>)
- **PostgreSQL** (<http://www.postgresql.org/lists.html>)

SANS Institute opublikował checklistę, która może zostać wykorzystana do wykonania audytu instalacji ORACLE :

<http://www.sans.org/score/oraclechecklist.php>

Center for Internet Security także opublikował **Oracle Database Benchmark Tool** do sprawdzania bezpieczeństwa Oracle:

http://www.cisecurity.org/bench_oracle.html

[SANS Security Oracle Step-by-Step](https://store.sans.org/store_item.php?item=80) zawiera przydatne informacje dotyczące konfiguracji i "utwardzania" instalacji Oracle:
(https://store.sans.org/store_item.php?item=80)

Na koniec, dodatkowe informacje o bezpieczeństwie baz danych dostępne są na stronach:

- SANS Reading Room on Database Security
(http://www.sans.org/rr/catindex.php?cat_id=3)
- <http://www.petefinnigan.com/orasec.htm>

[przejdź do początku dokumentu ^](#)

U10 Jądro

U10.1 Opis

Podstawowym komponentem systemu operacyjnego jest jego jądro. Jądro jest odpowiedzialne za szereg nisko poziomowych interakcji, pomiędzy systemem operacyjnym a sprzętem, pamięcią, komunikacją między procesową, systemem plików itp. Ponieważ jądro posiada przywileje umożliwiające dostęp do wszelkich aspektów systemu, kompromitacja na poziomie jądra ma poważne konsekwencje. Skutkiem może być denial of service, wykonanie dowolnego kodu z przywilejami systemu, nieograniczony dostęp do systemu plików, lub uprawnienia roota. Wiele luk może zostać wykorzystanych zdalnie. Mogą być niezwykle groźne, w sytuacji kiedy są wykorzystane za pomocą usługi która jest dostępna z poziomu Internetu. W niektórych przypadkach, wysłanie odpowiednio spreparowanego pakietu icmp może sprawić, że jądro się zapętli, zapychając tym samym wszystkie zasoby procesora w efekcie doprowadzając do zawieszenia usługi.

Odpowiednio skonfigurowane jądro nie tylko zapewni lepszą ochronę przed atakami, ale także wydajniejszą pracę systemu.

U10.2 Podatne systemy operacyjne

Właściwie wszystkie warianty systemu Unix, w tym Solaris, HP UX, dystrybucje Linux, BSD oraz systemy Windows posiadały w przeszłości luki na poziomie jądra.

U10.3 Wpisy CVE/CAN

[CVE-1999-0295](#), [CVE-1999-0367](#), [CVE-1999-0482](#), [CVE-1999-0727](#), [CVE-1999-0804](#),
[CVE-1999-1214](#), [CVE-1999-1339](#), [CVE-1999-1341](#), [CVE-2000-0274](#), [CVE-2000-0375](#),
[CVE-2000-0456](#), [CVE-2000-0506](#), [CVE-2000-0867](#), [CVE-2001-0062](#), [CVE-2001-0268](#),
[CVE-2001-0316](#), [CVE-2001-0317](#), [CVE-2001-0859](#), [CVE-2001-0993](#), [CVE-2001-1166](#),
[CVE-2002-0046](#), [CVE-2002-0766](#), [CVE-2002-0831](#)

[CAN-1999-1166](#), [CAN-2000-0227](#), [CAN-2001-0907](#), [CAN-2001-0914](#), [CAN-2001-1133](#),
[CAN-2001-1181](#), [CAN-2002-0279](#), [CAN-2002-0973](#), [CAN-2003-0127](#), [CAN-2003-0247](#),
[CAN-2003-0248](#), [CAN-2003-0418](#), [CAN-2003-0465](#), [CAN-2003-0955](#), [CAN-2003-0984](#),
[CAN-2004-0003](#), [CAN-2004-0010](#), [CAN-2004-0177](#), [CAN-2004-0482](#), [CAN-2004-0495](#),
[CAN-2004-0496](#), [CAN-2004-0497](#), [CAN-2004-0554](#), [CAN-2004-0602](#)

U10.4 Jak sprawdzić czy Twój system jest podatny na atak?

Istnieje szereg sposobów sprawdzenia, czy jądro systemu jest podatne na atak:

- jeżeli producent oferuje taką możliwość, należy zarejestrować celem otrzymywania informacji o uaktualnieniach bezpieczeństwa
- większość list dyskusyjnych dotyczących bezpieczeństwa rozprowadza informacje o lukach na poziomie jądra jak tylko są ogłaszane

- śledzenie wersji jądra uruchomionego na systemie powinno być częścią standardowych procedur bezpieczeństwa
- można wykorzystać skanery podatności, takie jak Nessus, do sprawdzenia podatnych wersji. Uwaga: niektóre z pluginów zawierających takie testy mogą spowodować zawieszenie się systemu, tak więc tego typu testy powinny być przeprowadzane bardzo ostrożnie

U10.5 Jak się przed tym chronić?

Istnieją dwie klasy parametrów, które mogą zostać wykorzystane do konfiguracji jądra w celu zapobiegnięcia atakom. Pierwsza klasa pozwala na ograniczenie podatności systemu na atak denial of service i ataków typu przepełnienie bufora. Druga klasa pozwala na „utwardzenie” jądra przed atakami sieciowymi. Polecenia i parametry są jednak zależne od konkretnego systemu operacyjnego. Należy więc dokładnie zapoznać się z dokumentacją jądra swojego systemu operacyjnego.

Zaleca się aby wszelkie modyfikacje przeprowadzać najpierw w środowisku testowym, zanim zostaną zaimplementowane w środowisku produkcyjnym, i że odpowiednie backup’y zostaną przeprowadzane na wypadek gdyby pojawiły się jakieś problemy.

Istnieje szereg przydatnych zasobów, opisujących jak konfigurować jądro systemowe:
[Solaris Tunable Parameters Reference Manual \(Solaris 8\)](#)
[Solaris Tunable Parameters Reference Manual \(Solaris 9\)](#)
[Solaris Operating Environment Network Settings for Security](#)
[Solaris Kernel Tuning for Security](#) or <http://www.securityfocus.com/infocus/1385>

[Linux Kernel Hardening](#)
[The Linux Kernel Archives](#)
[Linux Kernel Hardening](#)

[AIX Kernel Tuning](#)

[HP-UX Kernel Tuning and Performance Guide](#)

<http://docs.hp.com/hpux/pdf/5185-6559.pdf>
<http://docs.hp.com/hpux/pdf/TKP-90203.pdf>
<http://docs.hp.com/cgi-bin/otsearch/hpsearch>
<http://docs.hp.com/>

FreeBSD Handbook (zawiera informacje o kalibracji jądra):
http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/index.html

OpenBSD:
<http://www.openbsd.org/faq/index.html>
<http://www.openbsd.org/docum.html> (więcej informacji)

[NetBSD Tuning, Kernel Tuning](#)

[przejdź do początku dokumentu ^](#)

Dodatek A Lista portów które są często narażone na atak

W tej części prezentujemy listę często skanowanych i atakowanych portów. Ich blokada jest niezbędnym minimum w przypadku zabezpieczania brzegów sieci, ale nie stanowi pełnej specyfikacji konfiguracji firewalla. Znacznie lepszym podejściem jest blokada wszystkich niewykorzystywanych portów, tzn. blokowanie całego ruchu, a następnie odblokowanie konkretnych protokołów (niezbędnych do działalności organizacji) na wejściu do sieci.

Nawet jeżeli uważasz, że porty te są zablokowane, powinieneś aktywnie je monitorować w celu wykrycia prób włamań. Ostrzegamy, że zablokowanie niektórych z tych portów może spowodować zablokowanie niektórych niezbędnych usług. Prosimy dokładnie rozważyć potencjalne skutki zmian przed ich wprowadzeniem.

Uwaga: Należy jeszcze raz przypomnieć, że zaimplementowanie polityki domyślnej blokady usług i wpuszczania tylko tych niezbędnych jest powszechnie uznawane za skuteczniejszą metodę zabezpieczeń, niż blokowanie tylko wybranych portów. Podejście takie jest też bardziej przyjazne dla administratorów routerów i firewalli, gdyż listy konfiguracyjne i listy dostępu są w takim przypadku krótsze, bardziej logiczne i łatwiejsze w utrzymaniu.

Pamiętaj, że blokada tych portów nie jest działaniem zastępującym poprawną i rozległą politykę bezpieczeństwa. Nawet w przypadku gdy porty te zostaną zablokowane, atakujący, który uzyskał dostęp do Twojej sieci innymi metodami (np.: przez dial-up, załącznik e-maila z trojanem, atak z wewnątrz sieci lub skompromitowany host), może wykorzystać je do ataku, jeżeli usługi na nich rezydujące nie są odpowiednio zabezpieczone na każdym komputerze Twojej organizacji.

Nazwa	Port	Protokół	Opis
Small services	<20	tcp/udp	Tzw. small services
FTP	21	tcp	Transfer plików
SSH	22	tcp	Serwis login
TELNET	23	tcp	Serwis login
SMTP	25	tcp	Poczta
TIME	37	tcp/udp	Synchronizacja
WINS	42	tcp/udp	WINS
DNS	53	udp	System nazw
DNS zone transfers	53	tcp	System nazw
DHCP server	67	tcp/udp	Konfiguracja hosta
DHCP client	68	tcp/udp	Konfiguracja hosta
TFTP	69	udp	Różne
GOPHER	70	tcp	Stary odpowiednik WWW
FINGER	79	tcp	Różne
HTTP	80	tcp	WWW
alternate HTTP port	81	tcp	WWW
alternate HTTP port	88	tcp	WWW (czasem Kerberos)

LINUXCONF	98	tcp	Konfiguracja hosta
POP2	109	tcp	Poczta
POP3	110	tcp	Poczta
PORTMAP/RPCBIND	111	tcp/udp	RPC portmapper
NNTP	119	tcp	Wiadomości USENET
NTP	123	udp	Synchronizacja czasu
NetBIOS	135	tcp/udp	DCE-RPC endpoint mapper
NetBIOS	137	udp	NetBIOS name service
NetBIOS	138	udp	NetBIOS datagram service
NetBIOS/SAMBA	139	tcp	Udostępnianie plików przez sieć i serwis login
IMAP	143	tcp	Poczta
SNMP	161	tcp/udp	Różne
SNMP	162	tcp/udp	Różne
XDMCP	177	udp	X display manager protocol
BGP	179	tcp	Różne
FW1-secureremote	256	tcp	CheckPoint FireWall-1 mgmt
FW1-secureremote	264	tcp	CheckPoint FireWall-1 mgmt
LDAP	389	tcp/udp	System nazw
HTTPS	443	tcp	WWW
Windows 2000 NetBIOS	445	tcp/udp	SMB po IP (Microsoft-DS)
ISAKMP	500	udp	IPSEC Internet Key Exchange
REXEC	512	tcp	} trzy
RLOGIN	513	tcp	} Berkeley r-services
RSHELL	514	tcp	} (do zdalnego logowania)
RWHO	513	udp	Różne
SYSLOG	514	udp	Różne
LPD	515	tcp	Zdalne drukowanie
TALK	517	udp	Różne
RIP	520	udp	Protokół routingu
UUCP	540	tcp/udp	Transfer plików
HTTP RPC-EPMAP	593	tcp	HTTP DCE-RPC endpoint mapper
IPP	631	tcp	Zdalne drukowanie
LDAP over SSL	636	tcp	LDAP po SSL
Sun Mgmt Console	898	tcp	Zdalne zarządzanie
SAMBA-SWAT	901	tcp	Zdalna zarządzanie
Windows RPC programs	1025	tcp/udp	} często alokowane
Windows RPC programs	to		} przez DCE-RPC portmapper
Windows RPC programs	1039	tcp/udp	} na hostach Windows

SOCKS	1080	tcp	Różne
LotusNotes	1352	tcp	Baza danych/groupware
MS-SQL-S	1433	tcp	Baza danych
MS-SQL-M	1434	udp	Baza danych
CITRIX	1494	tcp	Remote graphical display
WINS replication	1512	tcp/udp	WINS
ORACLE	1521	tcp	Baza danych
NFS	2049	tcp/udp	NFS (dzielenie plików przez sieć)
COMPAQDIAG	2301	tcp	Compaq – zdalne zarządzanie
COMPAQDIAG	2381	tcp	Compaq – zdalne zarządzanie
CVS	2401	tcp	Dzielenie plików
SQUID	3128	tcp	Cache WWW
Global catalog LDAP	3268	tcp	Globalny katalog LDAP
Global catalog LDAP SSL	3269	tcp	Globalny katalog LDAP SSL
MYSQL	3306	tcp	Baza danych
Microsoft Term. Svc.	3389	tcp	Remote graphical display
LOCKD	4045	tcp/udp	NFS (dzielenie plików przez sieć)
Sun Mgmt Console	5987	tcp	Zdalne zarządzanie
PCANYWHERE	5631	tcp	Zdalne zarządzanie
PCANYWHERE	5632	tcp/udp	Zdalne zarządzanie
VNC	5800	tcp	Zdalne zarządzanie
VNC	5900	tcp	Zdalne zarządzanie
X11	6000- 6255	tcp	Serwer X Window
FONT-SERVICE	7100	tcp	Czcionki X Window
alternate HTTP port	8000	tcp	WWW
alternate HTTP port	8001	tcp	WWW
alternate HTTP port	8002	tcp	WWW
alternate HTTP port	8080	tcp	WWW
alternate HTTP port	8081	tcp	WWW
alternate HTTP port	8888	tcp	WWW
Unix RPC programs	32770	tcp/udp	} często przydzielane
Unix RPC programs	to		} przez RPC portmapper
Unix RPC programs	32899	tcp/udp	} na systemach Solaris
COMPAQDIAG	49400	tcp	Compaq – zdalne zarządzanie
COMPAQDIAG	49401	tcp	Compaq – zdalne zarządzanie
PCANYWHERE	65301	tcp	Zdalne zarządzanie

ICMP: blokuj przychodzące komunikaty „echo request” (ping i Windows traceroute), blokuj wychodzące „echo reply” oraz komunikaty „time exceeded” i „destination unreachable”, za wyjątkiem komunikatów typu „packet too big” (typ 3, kod 4). (Ten punkt zakłada, że jesteś gotów na rezygnację z normalnego wykorzystania zapytań

ICMP echo, w celu uniemożliwienia znanych nadużyć).

Poza powyższymi portami, zablokuj adresy spreparowane: pakiety przychodzące z zewnątrz, zawierające w nagłówku nadawcy wewnętrzne adresy z Twojej sieci, adresy prywatne (RFC1918) i adresy zarezerwowane przez IANA (patrz <http://www.iana.org/assignments/ipv4-address-space>). Zalecana jest blokada adresów typu broadcast lub multicast. Zalecane jest również blokowanie source routowanych pakietów bądź pakietów z ustawionymi flagami IP options.

Należy ustawić filtry na routerach brzegowych tak, aby blokowały sfalszowane pakiety wychodzące z Twojej sieci. Tylko pakiety wychodzące, których źródłem są adresy przypisane Twojej organizacji, powinny mieć możliwość przedostania się przez filtry.

Znaki towarowe: SANS Institute stara się uwzględnić w tym dokumencie kwestie związane z prawami intelektualnymi znakami towarowymi, prawami autorskimi, znakami usługowymi i patentami, . Wymienione poniżej produkty, systemy i aplikacje są objęte znakami towarowymi. Jeżeli uważasz, że pominęliśmy jakiś przypadek, wyślij e-mail ze swoimi uwagami na adres top20@sans.org.

Microsoft, Windows, Windows Server 2003, Microsoft SQL Server oraz Microsoft Outlook są znakami towarowymi lub zarejestrowanymi znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub innych krajach.

Sendmail jest znakiem towarowym lub zarejestrowanym znakiem towarowym Sendmail Inc w Stanach Zjednoczonych i/lub innych krajach.

SSH jest znakiem towarowym lub zarejestrowanym znakiem towarowym SSH Communication Security w Stanach Zjednoczonych i/lub innych krajach.

CERT Coordination Center jest znakiem towarowym lub zarejestrowanym znakiem towarowym Carnegie Mellon Software Engineering Institute w Stanach Zjednoczonych i/lub innych krajach.

UNIX jest znakiem towarowym lub zarejestrowanym znakiem towarowym The Open Group w Stanach Zjednoczonych i/lub innych krajach.

[przejdź do początku dokumentu](#) ^

Dodatek B

Eksperci, którzy pomogli stworzyć Listę 20 Największych Luk Bezpieczeństwa w Usługach w roku 2003

Adair Collins, US Department of Energy
Alan Paller, SANS Institute
Alex Lucas, United Kingdom National Infrastructure Security Co-ordination Center
Alexander Kotkov, CCH Legal Information Services
Anton Chuvakin, Ph.D., netForensics
BJ Bellamy, Kentucky Auditor of Public Accounts
Bradley Peterson, US Department of Energy
Cathy Booth, United Kingdom National Infrastructure Security Co-ordination Center - Incident Response CESG
Chris Benjes, National Security Agency

Christopher Misra, University of Massachusetts Amherst
Dave Dobrotka, Ernst & Young
Dominic Beecher, United Kingdom National Infrastructure Security Co-ordination
Ed Fisher, CableJiggler Consulting, LLC
Edward Skoudis, International Network Services
Edward W. Ray, MMICMAN LLC
Erik Kamerling, Pragmeta Networks/SANS Institute - Editor
Gerhard Eschelbeck, Qualys
Jeff Campione, Editor 2002
Jeff Ito, Indus Corporation
Jeni Li, Arizona State University
Kevin Thacker, United Kingdom National Infrastructure Security Co-ordination
Koon Yaw Tan, Infocomm Development Authority of Singapore (IDA)
Pedro Paulo Ferreira Bueno, MetroRED Telecom, Brazil
Pete Beck, United Kingdom National Infrastructure Security Co-ordination
Richard (Rick) Wanner, InfoSec Centre of Expertise (COE) CGI Information Systems & Management Consultants Inc.
Roland M Lascola, U.S. Dept. of Energy - Office of Independent Oversight and Performance Assurance
Ross Patel, Afentis Security
Russell Morrison, AXYS Environmental Consulting Ltd.
Scott A. Lawler, CISSP, Veridian Information Solutions
Stephen Northcutt, SANS Institute
Valdis Kletnieks, Virginia Tech
William Eckroade, U.S. Dept. of Energy

Podziękowania także dla następujących osób, które pomogły w edycji, składaniu i stworzeniu listy w 2003:

Audrey (Dalas) Bines, SANS Institute
Brian Corcoran, SANS Institute
Cara L. Mueller, SANS Institute

Podziękowania dla następujących absolwentów SANS za przegląd i komentarze dotyczące draftu listy w 2003 roku:

Paul Graham, CIT at the University at Buffalo (UB)
Jerry Berkman, UC Berkeley
Neil W Rickert, Northern Illinois University
Travis Hildebrand, US Department of Veteran Affairs
Christoph Gruber, WAVE Solutions
Mark Worthington, Affiliated Computer Services (ACS), Riverside Public Library
Matthew Nehawandian, CISSP

Eksperti, którzy pomogli stworzyć listę 20 Najbardziej Podatnych Usług w 2002 roku:

Jeff Campione, Federal Reserve Board - Editor
Eric Cole, Editor, 2001 Edition
Ryan C. Barnett, Department of the Treasury/ATF
Chris Benjes, National Security Agency
Matt Bishop, University of California, Davis

Chris Brenton, SANS Institute
Pedro Paulo Ferreira Bueno, Open Communications Security, Brazil
Anton Chuvakin, Ph.D., netForensics
Rob Clyde, Symantec
Dr. Fred Cohen, Sandia National Laboratories
Gerhard Eschelbeck, Qualys
Dan Ingevaldson, Internet Security Systems
Erik Kamerling, Pragmeta Networks
Gary Kessler, Gary Kessler Associates
Valdis Kletnieks, Virginia Tech CIRT
Alexander Kotkov - CCH Legal Information Services
Jamie Lau, Internet Security Systems
Scott Lawler, Veridias Information Solutions
Jeni Li, Arizona State University
Nick Main, Cerberus IT, Australia
Jose Marquez, Alutiq Security and Technology
Christopher Misra, University of Massachusetts
Stephen Northcutt, SANS Institute
Craig Ozancin, Symantec
Alan Paller, SANS Institute
Ross Patel, Afentis, UK
Marcus Ranum, ranum.com
Ed Ray - MMICMAN LLC
Chris Rouland, Internet Security Systems
Bruce Schneier, Counterpane Internet Security Inc.
Greg Shipley, Neohapsis
Ed Skoudis, Predictive Systems
Gene Spafford, Purdue University CERIAS
Koon Yaw Tan, Infocomm Development Authority of Singapore
Mike Torregrossa, University of Arizona
Viriya Upatising, Loxley Information Services, Thailand
Rick Wanner, CGI Information Systems and Management Consultants

Osoby, które pomogły określić priorytety wpisów CVE w celu zdefiniowania testów dla skanerów Top 20 w 2002 roku. Opis procesu selekcji znajduje się na stronie: www.sans.org/top20/testing.pdf

Charles Ajani, Standard Chartered Bank, London, UK
Steven Anderson, Computer Sciences Corporation, North Kingstown RI
John Benninghoff, RBC Dain Rauscher, Minneapolis MN
Layne Bro, BEA Systems, Denver CO
Thomas Buehlmann, Phoenix AZ
Ed Chan, NASA Ames Research Center, San Jose CA
Andrew Clarke, Computer Solutions, White Plains NY
Brian Coogan, ManageSoft, Melbourne Australia
Paul Docherty, Portcullis Computer Security Limited, UK
Arian Evans, U.S. Central Credit Union, Overland Park KS
Rich Fuchs, Research Libraries Group, Mountain View CA
Mark Gibbons, International Network Services, Minneapolis MN
Dan Goldberg, Rochester NY
Shan Hemphill, Sacramento CA
Michael Hensing, Charlotte, NC, Microsoft
Simon Horn, Brisbane Australia

Bruce Howard, Kanwal Computing Solutions, Jiliby NSW Australia
Tyler Hudak, Akron OH
Delbert Hundley, MPRI Division of L-3COM, Norfolk VA
Chyuan-Horng Jang, Oak Brook IL
Kim Kelly, The George Washington University, Washington DC
Martin Khoo, Singapore Computer Emergency Response Team (SingCERT), Singapore
Susan Koski, Pittsburgh PA
Kevin Liston, AT&T, Columbus OH
Andre Marien, Ubizen, Belgium
Fran McGowran, Deloitte & Touche, Dublin, Ireland, UK
Derek Milroy, Zurich North America, Chicago IL
Bruce Moore, Canadian Forces Network Operations Center, DND, Ottawa Canada
Castor Morales, Ft. Lauderdale FL
Luis Perez, Boston MA
Reg Quinton, University of Waterloo, Ontario Canada
Bartek Raszczyk, UWM Olsztyn, Olsztyn Poland
Teppo Rissanen, Plasec Oy, Helsinki Finland
Alan Rouse, N2 Broadband, Duluth GA
Denis Sanche, PWGSC ITSD/IPC, Hull, QC Canada
Felix Schallock, Ernst & Young, Vienna, Austria
Gaston Sloover, Fidelitas, Buenos Aires Argentina
Arthur Spencer, UMASS Medical School, Worcester MA
Rick Squires
Jeff Stehlin, HP
Koon Yaw TAN, Infocomm Development Authority of Singapore, Singapore
Steven Weil, Seitel Leeds & Associates, Seattle WA
Lance Wilson, Time Warner Cable/Broadband IS, Orlando FL
Andrew Wortman, Naval Research Laboratory, Washington DC
Carlos Zottman, Superior Tribunal de Justica, Brasilia Brazil

Pozostali eksperci od bezpieczenstwa sieciowego, którzy pomogli stworzyc liste Top 20 na rok 2001 i 2000, na bazie ktorej stworzono liste Top 20 2002.

Billy Austin, Intrusion.com
Phil Benchoff, Virginia Tech CIRT
Tina Bird, Counterpane Internet Security Inc.
Lee Brotzman, NASIRC Allied Technology Group Inc.
Mary Chaddock
Steve Christey, MITRE
Scott Conti, University of Massachusetts
Kelly Cooper, Genuity
Scott Craig, KMart
Sten Drescher, Tivoli Systems
Kathy Fithen, CERT Coordination Center
Nick FitzGerald, Computer Virus Consulting Ltd.
Igor Gashinsky, NetSec Inc.
Bill Hancock, Exodus Communications
Robert Harris, EDS
Shawn Hernan, CERT Coordination Center
Bill Hill, MITRE
Ron Jarrell, Virginia Tech CIRT
Jesper Johansson, Boston University
Christopher Klaus, Internet Security Systems

Clint Kreitner, Center for Internet Security
Jimmy Kuo, Network Associates Inc.
Jim Magdych, Network Associates Inc.
Dave Mann, BindView
Randy Marchany, Virginia Tech
Mark Martinec "Jozef Stefan" Institute
William McConnell, Trend Consulting Services
Peter Mell, National Institutes of Standards and Technology
Larry Merritt, National Security Agency
Mudge, @stake
Tim Mullen, AnchorIS.com
Ron Nguyen, Ernst & Young
David Nolan, Arch Paging
Hal Pomeranz, Deer Run Associates
Chris Prorise, Foundstone Inc.
Jim Ransome
RAZOR Research - BindView Development
Martin Roesch, Snort
Vince Rowe, FBI, NIPC
Marcus Sachs, JTF-CNO US Department of Defense
Tony Sager, National Security Agency
Gene Schultz, Lawrence Berkeley Laboratory
Eric Schultze, Foundstone
Derek Simmel, Carnegie Mellon University
Ed Skoudis, Predictive Systems
Lance Spitzner, Sun Microsystems, GESS Team
Wayne Stenson, Honeywell
Jeff Stutzman
Frank Swift
Bob Todd, Advanced Research Corporation
Jeff Tricoli, FBI NIPC
Laurie Zirkle, Virginia Tech CIRT

Eksperti którzy przyczynili się do powstania listy Top 20 w języku polskim:

Przemysław Jaroszewski, CERT Polska/NASK
Piotr Kijewski, CERT Polska/NASK
Jess Garcia, LAEFF/INTA

[przejdź do początku dokumentu ^](#)