



[zum Index der Top-20 Bedrohungen](#)

Einleitung

Die SANS Top 20 Internet Security Vulnerabilities

Vor vier Jahren veröffentlichten das SANS Institute, das National Infrastructure Protection Center (NIPC) und das FBI ein Dokument, in dem die 10 kritischsten Internet Sicherheitsschwachstellen beschrieben wurden. Tausende Organisationen haben dieses Dokument verwendet. Das Dokument wurde auf die Top 20 Sicherheitsschwachstellen erweitert und in den nächsten drei Jahren konnten damit die bedrohlichsten Sicherheitsprobleme behoben werden. Die sicherheitsrelevanten Services, die zu den Würmern wie Blaster, Slammer und Code Red geführt haben, waren in diesen Dokumenten beschrieben.

Das SANS Top-20 2005 Dokument weicht von den früheren Dokumenten ab. Zusätzlich zu den Kategorien Windows und UNIX wurden Cross-Platform Anwendungen und Netzwerk Produkte inkludiert. Diese Veränderung reflektiert die dynamische Natur der sich weiterentwickelnden Landschaft der Bedrohungen. Im Gegensatz zu den früheren Top-20 Listen ist diese Liste nicht kumulativ. Es wurden nur die Bedrohungen der letzten eineinhalb Jahre inkludiert. Wenn Sie Ihre Systeme schon länger nicht aktualisiert haben würden wir empfehlen, zuerst die Sicherheits-schwachstellen entsprechend der Liste des Jahres 2004 zu aktualisieren

Wir haben uns größte Mühe gegeben, damit die Liste für die meisten Organisationen sinnvoll ist. Folglich ist die Top-20 Liste ein Konsens von Schwachstellen, die sofort behoben werden sollen. Die Liste ist das Ergebnis von dutzenden führenden Sicherheitsexperten, die sicherheitsbewussten Regierungsbehörden aus GB, USA und Singapur stammen; weiters arbeiteten Spezialisten von führenden Herstellern von Sicherheitssoftware sowie Experten von Beratungsfirmen mit; Sicherheitsprogramme von Topuniversitäten waren ebenso involviert wie viele andere Organisationen und das SANS Institute. Eine detaillierte Liste der Mitwirkenden kann am Ende des Dokumentes gefunden werden.

Die SANS Top-20 Liste ist ein lebendes Dokument. In diesem Dokument sind Schritt-für-Schritt Anweisungen inkludiert sowie Hinweise, wo zusätzliche Informationen gefunden werden können, um Sicherheitsprobleme zu beheben. Wir werden diese Liste aktualisieren falls neue kritische Bedrohungen oder neue Lösungsansätze zur Behebung der Sicherheitsmängel bekannt werden. Ihr Input dazu ist willkommen. Dies ist ein , bzw. wenn bessere und einfachere Methoden zur Behebung der Sicherheitsschwachstellen bekannt werden. Diese Liste ist ein Gemeinschaftsdokument – ihre Erfahrung in der Bekämpfung und im Eliminieren der Sicherheitsschwachstellen kann anderen mit den gleichen Problemen helfen. Bitte senden Sie Vorschläge via E-Mail an top20@sans.org.

Top Schwachstellen in Windows Systemen

- W1. [Windows Services](#)
- W2. [Internet Explorer](#)
- W3. [Windows Libraries](#)
- W4. [Microsoft Office und Outlook Express](#)
- W5. [Windows Konfigurationsschwächen](#)

Top Schwachstellen in Cross-Platform Anwendungen

- C1. [Backup Software](#)
- C2. [AntiVirus Software](#)
- C3. [PHP-basierende Anwendungen](#)
- C4. [Datenbank Software](#)
- C5. [File Sharing Anwendungen](#)
- C6. [DNS Software](#)
- C7. [Media Player](#)
- C8. [Instant Messaging Anwendungen](#)
- C9. [Mozilla und Firefox Browsers](#)
- C10. [Weitere Cross-Platform Anwendungen](#)

Top Schwachstellen in UNIX Systemen

U1. [UNIX Konfigurationsschwächen](#)

U2. [Mac OS X](#)

Top Schwachstellen in Networking Produkte

N1. [Cisco IOS und nicht-IOS Produkte](#)

N2. [Juniper, CheckPoint und Symantec Produkte](#)

N3. [Cisco Devices Konfigurationsschwächen](#)

Top Schwachstellen in Windows Systemen

W1. Windows Services

W1.1 Beschreibung

Die Familie der Windows Betriebssysteme unterstützt eine Vielzahl von verschiedenen Services, Netzwerkmethoden und Technologien. Viele dieser Komponenten sind als Service Control Programme (SCP) implementiert und werden vom Service Control Manager (SCM) gesteuert, welcher Teil von Services.exe ist. Schwachstellen in diesen Services, die Betriebssystemfunktionalität implementieren, werden am häufigsten ausgenutzt.

Remote ausnutzbare Buffer Overflow Schwachstellen sind wieder die am meisten ausgenutzten Schwachstellen, die Windows Services betreffen. Viele der Core System Services stellen Remote Schnittstellen für Client Komponenten mittels Remote Procedure Calls (RPC) zur Verfügung. Durch Named Pipe Endpunkte, sowie durch bekannte und in manchen Fällen auch durch hohe TCP/UDP Ports sind diese Schnittstellen, die über das Common Internet File System (CIFS) Protokoll erreichbar sind, Bedrohungen ausgesetzt. Windows beinhaltet auch mehrere Services, die Netzwerkschnittstellen beinhalten, die auf einer Vielzahl von Protokollen basieren, darunter Internet Standards wie SMTP, NNTP, etc. Viele dieser Services können in anonymen Sessions verwendet werden, z.B. Sessions ohne Username und Kennwort und beliebiger Code kann mit "SYSTEM" Rechten ausgeführt werden.

Frühere Versionen des Betriebssystems, speziell Windows NT und Windows 2000, schalten diese Services automatisch bei standardmäßigen Installationen ein. Diese unwichtigen Services erhöhen die Gefahr eines Angriffes wesentlich.

Die folgenden kritischen Schwachstellen wurden für Windows Services letztes Jahr veröffentlicht:

- **MSDTC und COM+ Service** ([MS05-051](#))
- **Print Spooler Service** ([MS05-043](#))
- **Plug und Play Service** ([MS05-047](#), [MS05-039](#))
- **Server Message Block Service** ([MS05-027](#), [MS05-011](#))
- **Exchange SMTP Service** ([MS05-021](#))
- **Message Queuing Service** ([MS05-017](#))
- **License Logging Service** ([MS05-010](#))
- **WINS Service** ([MS04-045](#))
- **NNTP Service** ([MS04-036](#))
- **NetDDE Service** ([MS04-031](#))
- **Task Scheduler** ([MS04-022](#))

Exploits sind für die meisten Schwachstellen verfügbar. Der [Zotob Wurm](#) und verschiedene Varianten davon nutzen einen Buffer Overflow im Plug and Play Service. Bitte beachten Sie, dass die Patches MS05-047 und MS05-027 die Patches MS05-039 und MS05-011 ersetzen.

W1.2 Betroffene Betriebssysteme

Windows NT Workstation und Server, Windows 2000 Workstation und Server, Windows XP Home und Professional und Windows 2003 sind eventuell gefährdet.

W1.3 CVE Einträge

[CVE-2005-2120](#) , [CVE-2005-2119](#) , [CVE-2005-1984](#) , [CVE-2005-1983](#) , [CVE-2005-1978](#) , [CVE-2005-1206](#) , [CVE-2005-0045](#) , [CVE-2005-0560](#) , [CVE-2005-0059](#) , [CVE-2005-0050](#) , [CVE-2004-0567](#) , [CVE-2004-1080](#) , [CVE-2004-0574](#) , [CVE-2004-0206](#) , [CVE-2004-0212](#)

W1.4 Wie erkennt, ob man gefährdet ist

- Verwenden Sie einen [Vulnerability Scanner](#).
- Sie können auch überprüfen, ob Patches installiert wurden. Die Überprüfung erfolgt in der Registrierung im entsprechenden Schlüssel, der kann in der Registrierungsschlüssel Verifikation der entsprechenden Sicherheitsanweisung gefunden werden. Zusätzlich ist es wichtig sicher zu stellen, dass die aktualisierte Version der Dateien, die in der Sicherheitsanweisung beschrieben sind, in den Systemen installiert sind.
- Um zu überprüfen ob Ihr System für eine der Schwachstellen in den optionalen Services anfällig ist, müssen Sie überprüfen, ob das Service eingeschaltet ist. Das können Sie durch das Service Manager Interface tun, und zwar mit **Start->Ausführen** und dann tippen Sie **services.msc**. Die Reihe "Autostarttyp" zeigt ob die Dienste für automatischen Start konfiguriert sind

oder ob sie deaktiviert sind. Die Reihe "Status" im UI zeigt, ob der Dienst gestartet ist oder nicht.

W1.5 Wie man sich vor Windows Services Schwachstellen schützen kann

- Halten Sie die Systeme mit den letztgültigen Patches und Service Packs auf dem aktuellsten Stand. Wenn möglich aktivieren Sie die [Automatischen Updates](#) auf allen Systemen.
- Verwenden Sie [Intrusion Prevention/Detection Systeme](#) um sich gegen Angriffe zu schützen, die diese Schwachstellen ausnutzen.
- Stellen Sie fest, ob eine Schwachstelle für einen Dienst existiert, der entfernt werden kann. Wenn Ihr System zum Beispiel das Message Queuing Services ([CVE-2005-0059](#)) nicht benötigt, können Sie es in **Systemsteuerung -> Software -> Windows Komponenten hinzufügen/entfernen** entfernen. Seien Sie vorsichtig, wenn Sie das ausführen, da die Funktionalität beeinträchtigt werden kann, falls andere Software diese Dienste benötigt.
- In einigen Fällen können die Bedrohungen ausgeschaltet werden, indem die entsprechenden Dienste ausgeschaltet werden. Zum Beispiel kann das License Logging Service ([CVE-2005-0050](#)) in vielen Umgebungen ausgeschaltet werden. Tippen Sie **services.msc** im **Start->Ausführen** Menü um das Service Manager Interface zu starten. Finden Sie den entsprechenden Dienst und markieren Sie ihn, danach mit der rechten Maustaste anklicken. Selektieren Sie Eigenschaften in dem Menü. Der "Starttyp" kann ausgewählt werden und der Dienst kann deaktiviert werden.
- In einigen Fällen kann der Null Session Access zu dem entsprechenden Interface als "work-around" entfernt werden. Zum Beispiel kann die Spool-Schwachstelle ([CVE-2005-1984](#)) im Windows 2000 durch das Entfernen von SPOOLSS aus der Registrierung in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes entfernt werden. Es ist "best practice" die RestrictAnonymous Einstellungen zu überprüfen und die lokalen Einstellungen strikt einzustellen, je nach Ihrer Systemumgebung. <http://www.securityfocus.com/infocus/1352>
- Viele dieser Schwachstellen ([CVE-2005-1984](#), [CVE-2005-1983](#), [CVE-2005-1206](#), [CVE-2005-0045](#) etc) werden auf Schnittstellen gefunden die durch CIFS angeboten werden. Blockieren der Ports 139 und 445 an den Perimetergrenzen ist essenziell um remote Angriffe auszuschließen. Es ist auch "good practice" RPC Requests vom Internet auf Ports höher als 1024 zu blockieren, um Angriffe zu verhindern, die auf RPC Schwachstellen basieren, die Firewalls verwenden. (Ex: Message Queue [CVE-2005-0059](#)).
- XP SP2 und Windows 2003 SP1 haben verschiedene Sicherheitsverbesserungen, inklusive der Windows Firewall. Es wird empfohlen, zu diesen Versionen aufzugraden und die Firewall einzuschalten.

W1.6 Weiterführende Informationen

http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.aspx

http://www.microsoft.com/windows2000/en/advanced/help/sag_TCPIP_ovr_secfeatures.htm

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/4dbc4c95-935b-4617-b4f8-20fc947c7288.aspx>

a) Remote Code Ausführung in MSDTC und COM+ Services

<http://www.microsoft.com/technet/Security/bulletin/ms05-051.aspx>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely2>

b) Remote Code Ausführung im Print Spooler Service

<http://www.microsoft.com/technet/Security/bulletin/ms05-043.aspx>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=32#widely3>

c) Remote Code Ausführung im Plug and Play Service

<http://www.microsoft.com/technet/Security/bulletin/ms05-047.aspx>

<http://www.microsoft.com/technet/Security/bulletin/ms05-039.aspx>

<http://www.microsoft.com/security/incident/zotob.aspx>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=43#exploit1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=32#widely1>

<http://www.sans.org/newsletters/newsbites/newsbites.php?vol=7&issue=47#305>

d) Remote Code Ausführung im Server Message Block Service

<http://www.microsoft.com/technet/security/bulletin/ms05-027.aspx>

<http://www.microsoft.com/technet/security/bulletin/ms05-011.aspx>

<http://www.qualys.com/research/alerts/view.php/2005-06-14>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely6>

e) Remote Code Ausführung im Exchange SMTP Service

<http://www.microsoft.com/technet/security/Bulletin/MS05-021.aspx>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=16#exploit1>

f) Remote Code Ausführung im Message Queuing Service

<http://www.microsoft.com/technet/security/bulletin/ms05-017.aspx>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely2>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=19#exploit2>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=26#exploit2>

g) Remote Code Ausführung im License Logging Service

<http://www.microsoft.com/technet/security/bulletin/ms05-010.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=11#exploit1>

h) Remote Code Ausführung im WINS Service

<http://www.microsoft.com/technet/security/bulletin/MS04-045.msp>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=48#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=50#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=1#exploit1>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=2#exploit2>

i) Remote Code Ausführung im NNTP Service

<http://www.microsoft.com/technet/security/bulletin/MS04-036.msp>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely2>

j) Remote Code Ausführung im NetDDE Service

<http://www.microsoft.com/technet/security/bulletin/MS04-031.msp>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely4>

k) Remote Code Ausführung im Task Scheduler

<http://www.microsoft.com/technet/security/bulletin/ms04-022.asp>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely1>

W2. Internet Explorer

W2.1 Beschreibung

Der Microsoft Internet Explorer ist der am häufigsten verwendete Browser für das Internetsurfen und wird standardmäßig bei Windowssystemen installiert. Der Internet Explorer beinhaltet mehrere Schwachstellen, die zu Memory Corruption, Spoofing und der Ausführung von beliebigen Scripts führen kann. Die kritischsten Schwachstellen sind die, die zu Remote Code Ausführung führen, ohne dass der Anwender etwas dazu tun muss, außer eine dieser böartigen Webseiten zu öffnen oder E-Mail zu lesen. Exploit Code sind für viele dieser kritischen Schwachstellen verfügbar.

Diese Schwachstellen wurden weitgehend ausgenutzt, um Spyware, Adware oder anderen böartigen Code auf Anwendersystemen zu installieren. Die Spoofing Schwachstellen wurden verwendet, um Phishing Attacken durchzuführen. In vielen Fällen waren die Schwachstellen bekannt, bevor eine Lösung dafür verfügbar war.

Während der letzten Jahre hat Microsoft viele Updates für den Internet Explorer.

- a) Kumulativer Security Update für Internet Explorer ([MS05-052](#))
- b) Kumulativer Security Update für Internet Explorer ([MS05-038](#))
- c) JView Profile Remote Code Ausführung ([MS05-037](#))
- d) Kumulativer Security Update für Internet Explorer ([MS05-025](#))
- e) Kumulativer Security Update für Internet Explorer ([MS05-020](#))
- f) Kumulativer Security Update für Internet Explorer ([MS05-014](#))
- g) Windows Shell Remote Code Ausführung ([MS05-008](#))
- h) Kumulativer Security Update für Internet Explorer ([MS04-040](#))
- i) Kumulativer Security Update für Internet Explorer ([MS04-038](#))
- j) Kumulativer Security Update für Internet Explorer ([MS04-025](#))

Bitte beachten Sie, dass die letzten kumulativen Updates für den Internet Explorer alle vorigen Updates beinhalten.

W2.2 Betroffene Betriebssysteme

Internet Explorer 5.x und 6.x auf Windows 98/ME/SE, Windows NT Workstation und Server, Windows 2000 Workstation und Server, Windows XP Home und Professional und Windows 2003 sind potenziell betroffen.

W2.3 CVE Einträge

[CVE-2003-1048](#), [CVE-2004-0216](#), [CVE-2004-0549](#), [CVE-2004-0566](#), [CVE-2004-0727](#), [CVE-2004-0841](#), [CVE-2004-0842](#), [CVE-2004-](#)

[0843](#), [CVE-2004-0844](#), [CVE-2004-1050](#), [CVE-2005-0053](#), [CVE-2005-0054](#), [CVE-2005-0055](#), [CVE-2005-0056](#), [CVE-2005-0553](#), [CVE-2005-0554](#), [CVE-2005-0555](#), [CVE-2005-1211](#), [CVE-2005-1988](#), [CVE-2005-1989](#), [CVE-2005-1990](#), [CVE-2005-2087](#), [CVE-2005-2127](#)

W2.4 Wie erkennt, ob man gefährdet ist

- Verwenden Sie [Vulnerability Scanner](#).

W2.5 Wie man sich gegen diese Schwachstellen schützen kann

- Wenn Sie den Internet Explorer auf Ihren Systemen verwenden ist der beste Weg sich zu schützen, auf Windows XP Service Pack 2 zu aktualisieren. Die verbesserte Betriebssystemsicherheit und die Windows Firewall helfen, das Risiko zu verringern. Falls es nicht möglich ist, auf Windows XP Service Pack 2 zu aktualisieren sollten Sie einen anderen Browser verwenden.
- Halten Sie die Systeme aktuell und installieren Sie die letztgültigen Patches und Service Packs. Wenn möglich, aktivieren Sie die [Automatischen Updates](#) auf allen Systemen.
- Um Remote Exploits auf Administratorlevel zu verhindern, können die Anwender mit Microsofts [DropMyRights](#) den Internet Explorer mit "least privileges" betreiben.
- Viele Spyware Programme werden als Browser Helper Objects auf den Systemen installiert. Ein Browser Helper Object oder BHO ist ein kleines Programm, das automatisch ausgeführt wird, wenn der Internet Explorer gestartet wird und die Funktionalität erweitert. Browser Helper Objects können mit AV Scannern erkannt werden. Eine andere Möglichkeit ist die periodische Überprüfung der BHOs mit [BHO-Daemon](#) oder [Microsoft AntiSpyware](#).
- Verwenden Sie [Intrusion Prevention/Detection Systems](#) und [Anti-virus und Malware Detection Software](#) um bösartigen HTML Script Code zu entfernen.

W2.6 Wie man den Internet Explorer sicherer konfigurieren kann

Um die Sicherheitseinstellungen für den Internet Explorer zu konfigurieren:

- Wählen Sie Internetoptionen unter dem Menüpunkt Extras.
- Wählen Sie Sicherheit und dann klicken Sie auf "Stufe anpassen" für die Internet Zone.
- Die meisten Probleme im IE werden durch Active Scripting oder ActiveX Steuerelemente verursacht.
- Unter Scripting wählen Sie Einfügeoperation über ein Script zulassen, klicken Sie auf Deaktivieren um zu verhindern, dass Content vom Clipboard ausgelesen werden kann.
 - **Hinweis:** Wenn Sie Active Scripting deaktivieren, können einige Webseiten nicht mehr richtig funktionieren. ActiveX Steuerelemente sind nicht so populär aber gefährlicher, da die Steuerelemente höheren Zugang zu den Systemen erlaubt.
- Wählen Sie Deaktivieren für signierten und unsignierten ActiveX Steuerelementen. Wählen Sie ebenfalls Deaktivieren für ActiveX Steuerelemente initialisieren und ausführen, die nicht sicher sind.
- Java Applets haben üblicherweise mehr Möglichkeiten als Scripts. Unter Microsoft wählen Sie Hohe Sicherheit für Java Einstellungen um Java Applets ordentlich in einer Sandbox auszuführen um privilegierten Access zu den Systemen zu verhindern.
- Unter Verschiedenes wählen Sie Deaktivieren für den Punkt Auf Datenquellen über Domaingrenzen hinweg zugreifen um Cross-site Scripting Attacken zu vermeiden.
- Bitte stellen Sie auch sicher, dass keine eingeschränkten Sites unter Vertrauenswürdigen Sites oder lokales Intranet eingetragen sind, da diese Zonen schwächere Sicherheitseinstellungen haben als die anderen Zonen.

W2.7 Weiterführende Informationen

Internet Explorer Security Updates

- a) <http://www.microsoft.com/technet/security/Bulletin/MS05-052.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely3>
- b) <http://www.microsoft.com/technet/security/Bulletin/MS05-038.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=32#widely2>
- c) <http://www.microsoft.com/technet/security/Bulletin/MS05-037.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=28#widely1>
- d) <http://www.microsoft.com/technet/security/Bulletin/MS05-025.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely1>
- e) <http://www.microsoft.com/technet/security/Bulletin/MS05-020.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely3>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=17#exploit2>
- f) <http://www.microsoft.com/technet/security/bulletin/ms05-014.msp>
<http://www.microsoft.com/technet/security/bulletin/ms05-008.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely2>
- g) <http://www.microsoft.com/technet/security/bulletin/MS04-040.msp>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=48#widely2>
- h) <http://www.microsoft.com/technet/security/bulletin/MS04-038.msp>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely1>

- i) <http://www.microsoft.com/technet/security/bulletin/MS04-025.msp>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=30#widely1>

Internet Explorer 0-day Schwachstellen (zur Zeit der Entdeckung der Schwachstelle)

<http://www.sans.org/newsletters/risk/display.php?v=4&i=33#widely3>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=29#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=26#widely2>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=27#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=51#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=51#widely4>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=52#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=46#widely2>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=45#widely4>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=44#widely2>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=43#widely2>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=44#widely3>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=42#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=43#widely2>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=34#exploit1>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=33#widely1>
<http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely2>

W3. Windows Libraries

W3.1 Beschreibung

Windows Anwendungen verwenden eine große Anzahl von System Libraries, die oft in DLL Dateien gepackt sind. Diese Libraries werden für viele Tasks verwendet, wie zum Beispiel HTML Parsing, Bildformat Decoding, etc. Lokal wie Remote anwendbare Programme verwenden diese Libraries. Daher haben kritische Schwachstellen in einer Library üblicherweise Auswirkungen auf eine Vielzahl von Microsoft und Drittanbieter Programmen, die diese Library verwenden. Exploits können oft auf unterschiedlichen Weisen ausgenutzt werden. Zum Beispiel kann ein Exploit in einer Bildverarbeitenden Library im Internet Explorer, im Office und in Image Viewern ausgenutzt werden. In den meisten Fällen werden die Libraries in allen möglichen Windows Betriebssystemversionen verwendet, wodurch die Anzahl der möglichen Angriffsziele vervielfacht wird.

Kritische Libraries, die während des letzten Jahres betroffen waren:

- (a) Windows Graphics Rendering Engine Remote Code Ausführung ([MS05-053](#))
- (b) Microsoft DirectShow Remote Code Ausführung ([MS05-050](#))
- (c) Microsoft Color Management Module Remote Code Ausführung ([MS05-036](#))
- (d) HTML Help Remote Code Ausführung ([MS05-026](#), [MS05-001](#), [MS04-023](#))
- (e) Web View Remote Code Ausführung ([MS05-024](#))
- (f) Windows Shell Remote Command Ausführung ([MS05-049](#), [MS05-016](#), [MS04-037](#), [MS04-024](#))
- (g) Windows Hyperlink Object Library Remote Code Ausführung ([MS05-015](#))
- (h) PNG Image Processing Remote Code Ausführung ([MS05-009](#))
- (i) Cursor und Icon Processing Remote Code Ausführung ([MS05-002](#))
- (j) Windows Compressed Folder Remote Code Ausführung ([MS04-034](#))
- (k) JPEG Processing Remote Code Ausführung ([MS04-028](#))

Für die meisten Schwachstellen sind Exploit Code öffentlich verfügbar. Automatische Angriffe die diese Schwachstellen ausnutzen wurden bereits im Internet gefunden. Ein Beispiel für eine groß angelegte Attacke involvierte die Ausnutzung eines Cursor und Icon Handhabungsfehlers, um Malware auf den Anwendersystemen zu installieren. Der Trojaner [Phel.A](#) nutzt eine Schwachstelle in der HTML Help Library aus. Wichtig ist, dass einige Libraries wie HTML Help und Windows Shell beinhalten die älteren Updates in den neueren Updates, daher müssen nur die neuesten Updates installiert werden.

W3.2 Betroffene Betriebssysteme

Windows NT 4, Windows 2000, Windows XP, Windows 2003

W3.3 CVE Einträge

[CVE-2003-1041](#), [CVE-2004-0201](#), [CVE-2004-0200](#), [CVE-2004-0214](#), [CVE-2004-0420](#), [CVE-2004-0575](#), [CVE-2004-0597](#), [CVE-2004-1043](#), [CVE-2004-1049](#), [CVE-2004-1244](#), [CVE-2005-0057](#), [CVE-2005-0063](#), [CVE-2005-1191](#), [CVE-2005-1208](#), [CVE-2005-1219](#), [CVE-2005-2117](#), [CVE-2005-2118](#), [CVE-2005-2122](#), [CVE-2005-2123](#), [CVE-2005-2124](#), [CVE-2005-2128](#)

W3.4 Wie erkennt, ob man gefährdet ist

Diese Fehler können am besten gelöst werden, in dem man die Systeme aktualisiert, da work-arounds kompliziert sind, da es verschiedenen Angriffspunkte geben kann. Man kann [Vulnerability Scanners](#) verwenden um festzustellen, ob die Updates installiert sind.

W3.5 Wie man sich vor Schwachstellen in Windows Libraries schützen kann

- Stellen Sie sicher, dass die Windows Systeme die letzten Sicherheitspatches installiert hat.
- Blockieren Sie an der Netzwerkgrenze die Ports 135-139/TCP, 445/TCP und andere Ports, die von Windows verwendet werden. Dies schützt vor Remote Angreifern die diese Schwachstellen via Shared File System ausnützen könnten.
- Verwenden Sie TCP/IP Filter, die in Windows 2000 und XP verfügbar sind, oder die Internet Connection Firewall in Windows XP Systeme um inbound Zugriff auf die betroffenen Ports zu vermeiden. Die Verwendung einer ordentlich konfigurierten Personal/ Netzwerk Firewall löst dieses Problem ebenfalls.
- Aufgrund der Vielzahl von Angriffsmöglichkeiten sind [Intrusion Prevention/Detection Systems](#) und [Anti-virus und Malware Detection Software](#) sehr hilfreich um sich vor den Gefahren dieser Schwachstellen zu schützen.
- Wenn Sie eine Anwendung einer Drittfirma auf kundenspezifischen Windows 2000/XP Systemen betreiben stellen Sie sicher, dass auch die Updates der Software der Drittfirma installiert wurden.
- Beachten Sie das Prinzip der "geringsten Rechte" um zu minimieren, dass Würmer und Trojaner sich auf anderen Systemen ausbreiten. Zusätzliche Details zur Minimierung des Zugriffs auf bestimmte Registrierungsschlüssel, ausführbare Dateien und Verzeichnisse können in dem NSA Guide <http://www.nsa.gov/snac/index.cfm?MenuID=scg10.3.1> gefunden werden.
- Verwenden sie Systemhärtungsrichtlinien (wie die von [ClSecurity](#)) um die Systeme resistenter gegen Remote oder lokale Angriffe zu machen.

W3.6 Weiterführende Informationen

Microsoft Graphics Rendering Engine Remote Code Ausführung

<http://www.microsoft.com/technet/security/Bulletin/MS05-053.msp> <http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely1>

Microsoft DirectShow Remote Code Ausführung

<http://www.microsoft.com/technet/security/Bulletin/MS05-050.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=41#widely1>

Microsoft Color Management Module Remote Code Ausführung

<http://www.microsoft.com/technet/security/Bulletin/MS05-036.msp> <http://www.sans.org/newsletters/risk/display.php?v=4&i=28#widely2> <http://www.sans.org/newsletters/risk/display.php?v=4&i=29#exploit1>

HTML Help Remote Code Ausführung

<http://www.microsoft.com/technet/security/bulletin/MS05-026.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely2>
<http://www.microsoft.com/technet/security/bulletin/MS05-001.msp>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=2#widely1>

<http://www.microsoft.com/technet/security/bulletin/MS04-023.msp>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely3>

Web View Remote Code Ausführung

<http://www.microsoft.com/technet/security/bulletin/MS05-024.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=19#widely2>

Windows Shell Remote Command Ausführung

<http://www.microsoft.com/technet/security/bulletin/MS05-016.msp>
<http://www.sans.org/newsletters/risk/display.php?v=4&i=15#widely6>

<http://www.microsoft.com/technet/security/bulletin/MS04-037.msp>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely5>

<http://www.microsoft.com/technet/security/bulletin/MS04-024.msp> <http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely5>

Windows Hyperlink Object Library Remote Code Ausführung

<http://www.microsoft.com/technet/security/bulletin/ms05-015.msp> <http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely10>

PNG Image Processing Remote Code Ausführung

<http://www.microsoft.com/technet/security/bulletin/ms05-009.msp>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely>

Cursor und Icon Processing Remote Code Ausführung

<http://www.microsoft.com/technet/security/bulletin/ms05-002.msp> <http://www.sans.org/newsletters/risk/display.php?v=4&i=2#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=51#widely2>

Windows Compressed Folder Remote Code Ausführung

<http://www.microsoft.com/technet/security/bulletin/MS04-034.msp> <http://www.sans.org/newsletters/risk/display.php?v=3&i=41#widely3>

JPEG Processing Remote Code Ausführung

<http://www.microsoft.com/technet/security/bulletin/MS04-028.msp> <http://www.sans.org/newsletters/risk/display.php?v=3&i=37#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=38#widely2>

W4. Microsoft Office und Outlook Express

W4.1 Beschreibung

Microsoft Office ist die am häufigsten verwendete E-Mail Anwendung und Office Suite weltweit. Die Anwendungen Outlook, Word, Powerpoint, Excel, Visio, Frontpage, Access usw. sind beinhaltet. Bitte beachten Sie, dass Outlook Express, ein einfacher E-Mail Client ist auf allen Versionen von Microsoft Windows seit Windows 95 installiert. Schwachstellen in diesen Produkten können unter folgenden Szenarien ausgenutzt werden:

- Der Angreifer sendet ein bösartiges Office Dokument in einer E-Mail. Viren können diese Schwachstelle ausnutzen.
- Der Angreifer hostet ein Dokument auf einem Webserver oder in einem Verzeichnis und lockt einen Anwender auf die Webseite oder zu dem Verzeichnis. Bitte beachten Sie, dass der Windows Explorer Office Dokumente automatisch öffnet. Daher genügt es, dass eine Webseite oder ein Verzeichnis geöffnet wird, um diese Schwachstellen auszunutzen.
- Der Angreifer betreibt einen Server wie einen News Server, der bösartige Antworten sendet um einen Buffer Overflow im E-Mail Client verursacht.

Die kritischen Probleme, die im letzten Jahr für Office und Outlook Express veröffentlicht wurden:

a) **Kumulativer Security Updates für Outlook Express** ([MS05-030](#))

b) **Microsoft OLE und COM Remote Code Ausführung** ([MS05-012](#))

c) **Microsoft Office XP Remote Code Ausführung** ([MS05-005](#))

Exploit Code und technische Details sind für diese Schwachstellen öffentlich verfügbar. Für den Fehler im Office Access Komponenten ist noch immer kein Patch verfügbar und diese Schwachstelle wird von Trojanern ausgenutzt.

W4.2 Betroffene Betriebssysteme

Windows NT Workstation und Server, Windows 2000 Workstation und Server, Windows XP Home und Professional und Windows 2003 sind potenziell betroffen.

W4.3 CVE Einträge

[CVE-2004-0848](#) , [CVE-2005-0044](#) , [CVE-2005-1213](#)

W4.4 Wie erkennt, ob man gefährdet ist

Die Office und Outlook Express Installationen, die ohne die Patches, die in den oben angegebenen Microsoft Bulletins betrieben werden, sind gefährdet. Die einfachste Möglichkeit ist die Verwendung eines [Vulnerability Scanners](#).

W4.5 Wie man sich gegen diese Schwachstellen schützen kann

- Halten Sie die Systeme mit den letztgültigen Patches und Service Packs auf dem aktuellsten Stand. Wenn möglich aktivieren Sie die [Automatischen Updates](#) auf allen Systemen.
- [Deaktivieren](#) Sie das Internet Explorer Features, dass Office Dokumente automatisch geöffnet werden.
- Konfigurieren Sie Outlook und Outlook Express mit erweiterten [Sicherheitsoptionen](#).
- Verwenden Sie [Intrusion Prevention/Detection Systeme](#) und [Anti-virus und Malware Detection Software](#), um die Anwender vor schädigenden Antworten von bösartigen Servern zu schützen.

W4.6 Weiterführende Informationen

a) Microsoft Office XP Buffer Overflow

<http://www.microsoft.com/technet/Security/bulletin/ms05-005.msp>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely4>

b) Microsoft OLE und COM Remote Code Ausführung

<http://www.microsoft.com/technet/Security/bulletin/ms05-012.msp>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely7>

c) Kumulative Security Updates für Outlook Express

<http://www.microsoft.com/technet/security/bulletin/ms05-030.msp>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=26#exploit3>

d) Office Access Buffer Overflow (noch kein Patch vorhanden)

<http://www.sans.org/newsletters/risk/display.php?v=4&i=15#exploit1>

<http://securityresponse.symantec.com/avcenter/venc/data/backdoor.ryejet.b.html>

W5. Windows Konfigurationsschwächen

W5.1 Beschreibung

Die Konfigurationsschwachstellen in Windows Systemen werden noch immer von neuen „bots“ und Würmern ausgenutzt. Diese Schwachstellen werden typischerweise in folgende Kategorien geteilt:

Schwache Kennwörter für Windows Accounts oder Netzwerk-Shares

In den letzten Jahren waren die schwachen Authentifizierungsmethoden in Windows unter den "Top 10" Windowsschwachstellen. LAN Manager (LM) Hashes sind als schwach bekannt und wurden durch verschiedene Versionen von NTLM (NTLM und NTLMv2) Authentifizierungen ersetzt. Obwohl die aktuellen Windowsversionen keine Notwendigkeit für LAN Manager (LM) Unterstützung haben, speichert Microsoft Windows standardmäßig lokal LM Kennwort-Hashes (auch bekannt als LANMAN Hashes) bei Windows NT, 2000 und XP Systemen (nicht bei Windows 2003).

Die LM Verschlüsselungsmethoden sind schwächer als die aktuelle Microsoftverschlüsselungen (NTLM and NTLMv2) und können in relativ kurzer Zeit von Angreifern entschlüsselt werden. Selbst Kennwörter, die eigentlich als starke Kennwörter gelten, können mit „brute-force“ Attacken mit der zur Zeit verfügbaren Hardware in weniger als einer Woche entschlüsselt werden. Ein Angreifer kann entweder bekannte Standardkennwörter, „brute force“ Attacken oder "dictionary" Attacken verwenden, um das Kennwort eines User-Accounts zu entschlüsseln. Programme wie THC's Hydra können verwendet werden, um Remote Kennwörter zu entschlüsseln. L0phtCrack und John the Ripper sind bekannte Kennwortkrackprogramme oder Auditprogramme.

Viele Familien von Würmern oder BOT Zombies wie GaoBot, PhatBot und AgoBot verbreiten sich über Netzwerk-Shares, die schwache Kennwörter verwenden. Diese Würmer verwenden eine Liste von hardcoded Kennwörtern, die mit den Kennwörtern der Opfer verglichen werden und wenn eine Übereinstimmung gefunden wird, verbreiten sie sich.

Standardmäßige Konfiguration/Kennwörter für Server

Bei der Installation der Microsoft Data Engine (MSDE) oder des Microsoft SQL Server Desktop (MSDE2000) hat der standard SQL Administrator Account oder "sa" Account ein leeres Kennwort und verwendet die SQL Authentifizierung. MSDE kommt als eine Komponente von verschiedenen Anwendungen, wie Microsoft Office 2000 und anderen „third party“ Anwendungen. Dieses leere oder Null Kennwort ist anfällig für einen Wurm. Zum Beispiel haben die Würmer Voyager Alpha Force, SQL Spida und Cblade diese Schwachstelle ausgenutzt.

IIS Server Standardeinstellungen sind ebenfalls anfällig für Angriffe. Einige Accounts, die standardmäßig kreiert werden, z.B. IUSR_Computername Account haben Schreibrechte selbst für anonyme User. Die Rechte für solche Accounts sollen eingeschränkt werden, um den Zugang einzuschränken.

IIS Service wie FTP, NNTP oder SMTP sind standardmäßig aktiviert und bieten ein gutes Angriffsziel. Diese Service sollten deaktiviert werden.

W5.2 Betroffene Betriebssysteme

Windows NT, Windows 2000, Windows XP und Windows 2003

W5.3 Wie man sich gegen diese Schwachstellen schützen kann

- Setzen Sie starke Kennwort Policies ein, Kennwörter sollen ein Minimum an Zeichen haben (mindestens 12, wenn möglich). Verwenden Sie Programme wie L0phtcrack oder John The Ripper um Accounts mit schlechten Kennwörtern zu überprüfen.
- Vermeiden Sie, dass Windows LM Hash in Active Directory oder in der SAM Datenbank verwendet, verwenden Sie dazu die von Microsoft veröffentlichten [Instruktionen](#).
- [Optimieren Sie die Registrierung](#) um anonymen Zugriff auf Netzwerk-Shares zu verhindern.
- Modifizieren Sie die Standardkonfigurationseinstellungen in IIS Servern und MS-SQL Servern.

W5.4 Weiterführende Informationen

GaoBot Information

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

Brute force scannen gegen MS SQL Serveraccounts; Sind Sie paranoid genug?

<http://isc.sans.org/diary.php?date=2004-12-30>

Unsichere SQL Server mit Blank (NULL) SA Kennwörtern bieten Würmern eine Angriffsmöglichkeit

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q313418>

CERT Vulnerability Note

<http://www.kb.cert.org/vuls/id/635463>

IIS 6.0 Security Best Practices

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/596cdf5a-c852-4b79-b55a-708e5283ced5.msp>

Wie verwendet man die RestrictAnonymous Registrierungswerte in Windows 2000

<http://support.microsoft.com/kb/q246261>

Top Vulnerabilities in Cross-Platform Anwendungen

C1. Backup Software

C1.1 Beschreibung

Backup Software ist eine wertvolle Anlage für jede Organisation. Die Software läuft üblicherweise auf eine großen Anzahl von Systemen in einem Unternehmen. In den letzten Jahren und mit dem Wachstum der Daten wurde ein Trend festgestellt, die Backup Funktionalität auf wenige Server oder sogar nur auf einen einzelnen Backup Server zu konsolidieren. Die Hosts die das Backup Service beanspruchen kommunizieren über das Netzwerk mit dem Backup Server. Das kann mittels Push Funktionalität geschehen – ein Client sendet Daten zu einem Server – oder durch Push Funktionalität – der Server verbindet sich zu dem Client – oder eine Kombination von beiden. Während des letzten Jahren wurden einige kritische Sicherheitsschwachstellen in Backup Software entdeckt. Diese Schwachstellen können ausgenutzt werden um den Server, der die Backup Software ausführt total zu kompromittieren und/oder den Backup Client. Ein Angreifer kann diese Fehler wirksam einsetzen und eine unternehmensweite Kompromittierung erzielen, indem er Zugang zu den sensiblen Backupdaten erhält. Exploits wurden schon veröffentlicht und mehrere automatisierte Angriffsprogramme verwenden die veröffentlichten Exploitcode.

C1.2 Betroffene Betriebssysteme und Backup Software

Alle Betriebssysteme, die Backup Server oder Backup Client Software ausführen sind potenziell gefährdet. Die betroffenen Betriebssysteme sind vorwiegend Windows und UNIX Systeme.

Die folgenden weitverbreiteten Software Pakete sind bekannt als anfällig für diese Schwachstellen

- Symantec Veritas NetBackup/Backup Exec
- Symantec Veritas Storage Exec
- Computer Associates BrightStor ARCserve
- EMC Legato Networker
- Sun StorEdge Enterprise Backup Software (formerly Solstice Backup Software)
- Arkeia Network Backup Software
- BakBone Netvault Backup Software

C1.3 CVE Einträge

[CVE-2004-1172](#), [CVE-2004-1389](#), [CVE-2005-0260](#), [CVE-2005-0349](#), [CVE-2005-0357](#), [CVE-2005-0358](#), [CVE-2005-0491](#), [CVE-2005-0496](#), [CVE-2005-0581](#), [CVE-2005-0582](#), [CVE-2005-0583](#), [CVE-2005-0771](#), [CVE-2005-0773](#), [CVE-2005-1009](#), [CVE-2005-1019](#), [CVE-2005-1272](#), [CVE-2005-1547](#), [CVE-2005-2051](#), [CVE-2005-2079](#), [CVE-2005-2080](#), [CVE-2005-2535](#), [CVE-2005-2611](#), [CVE-2005-2715](#), [CVE-2005-2996](#), [CVE-2005-3116](#)

-

-

C1.4 Wie erkennt, ob man gefährdet ist

- Verwenden Sie [Vulnerability Scanner](#) um fehlerhafte Backup Software Installationen zu finden.
- Wenn Sie Backup Software verwenden, die vorher beschrieben wurde wird empfohlen, die letztgültigen Patches und Versionen zu installieren. Überprüfen Sie die Backup Software Site des Herstellers und abonnieren Sie die Patch Benachrichtigungen wenn verfügbar und besuchen Sie regelmäßig einige der allgemein bekannten Sicherheitssites wie [US-CERT](#), [CERT](#), [SANS](#), um neue Schwachstellenankündigungen für die von Ihnen verwendete Backup Software zu finden.
- Die typische Ports, die Backup Software verwenden:

Symantec Veritas Backup Exec

TCP/10000 TCP/8099, TCP/6106

Eine Liste von Ports der Veritas Backup Daemons finden Sie [hier](#).

CA BrightStor ARCserve Backup Agent

TCP/6050, UDP/6051, TCP/6070, TCP/41523, UDP/41524

Sun und EMC Legato Networker

TCP/7937-9936

Arkeia Network Backup

TCP/617

BakBone Netvault Backup

C1.5 Wie man sich gegen diese Schwachstellen schützt

- Stellen Sie sicher, dass die letztgültigen Hersteller Patches auf Client und Server installiert sind.
- Die Ports, die von der Backup Software verwendet werden, sollen mittels einer Firewall von unsicheren Netzwerken inklusive Internet gesperrt werden.
- Daten sollten verschlüsselt auf Backup Medien gespeichert werden und während des Transportes über das Netzwerk verschlüsselt werden.
- Host/Netzwerk basierende Firewalls sollten installiert werden, um den Zugriff auf Systeme mit Backup Software zu limitieren und um sicher zu stellen, dass nur die richtigen Backup Hosts mit den Backup Servern kommunizieren können.
- Teilen Sie das Netzwerk und verwenden Sie einen eigenen Backupnetzwerk VLAN.
- Backup Medien sollen aufbewahrt, ausgewiesen und gefunden werden, wie andere IT Assets, um Diebstahl und Verlust zu verhindern.
- Backup Medien sollen nach dem Ende des Life-Cycles sicher gelöscht oder physisch zerstört werden.

C1.6 Weiterführende Informationen

Computer Associates Advisories

- <http://archives.neohapsis.com/archives/bugtraq/2005-08/0033.html>
- <http://archives.neohapsis.com/archives/bugtraq/2005-04/0202.html>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=31#widely1>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=15#other1>
- http://www.ca.com/at/local/partner/techtalk_mar05_faq.pdf (Ports verwendet von Backup Produkten)

Symantec Veritas Advisories

- <http://seer.support.veritas.com/docs/279553.htm>
- <http://seer.support.veritas.com/docs/276604.htm>
- <http://seer.support.veritas.com/docs/276605.htm>
- <http://seer.support.veritas.com/docs/276606.htm>
- <http://seer.support.veritas.com/docs/276533.htm>
- <http://seer.support.veritas.com/docs/276607.htm>
- <http://seer.support.veritas.com/docs/277567.htm>
- <http://seer.support.veritas.com/docs/277566.htm>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely4>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=38#other3>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely1>
- http://www.us-cert.gov/current/current_activity.html#VU378957

EMC Legato und Sun Advisories

- http://www.legato.com/support/websupport/product_alerts/081605_NW_token_authentication.htm
- http://www.legato.com/support/websupport/product_alerts/081605_NW_authentication.htm
- <http://sunsolve.sun.com/search/document.do?assetkey=1-26-101886-1>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=33#widely2>

Arkeia Advisory

- <http://www.arkeia.com/securityfix/>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=8#widely1>

BakBone Advisory

- <http://www.sans.org/newsletters/risk/display.php?v=4&i=19#other1> (unpatched)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=14#other1>

C2. Anti-virus Software

C2.1 Beschreibung

AntiVirus Software wird als Basiswerkzeug innerhalb der "defense-in-depth" Toolbox gesehen, um die Systeme gegen die heutigen Bedrohungen zu schützen. AntiVirus Software ist jetzt fast auf allen Desktops, Servern und Gateways auf unterschiedlichen Plattformen installiert um Virenausbrüche zu verhindern.

Während des letzten Jahres wurde eine Veränderung bemerkt, um Sicherheitsprodukte, die von vielen Unternehmen und Endusern verwendet werden, auszunutzen. Das inkludiert AntiVirus Produkte und Personal Firewall Software. Die Entdeckung von Schwachstellen in AntiVirus Software ist nicht beschränkt auf Desktop und Server Plattformen. Gateway Lösungen können ebenfalls

betroffen sein. Die Kompromittierung eines Gateways kann eine wesentlich größere Auswirkung haben, da diese Gateways ist der äußerste Schutz und oft auch der einzige Schutz in vielen kleinen Organisationen.

Mehrere Buffer Overflow Schwachstellen wurden in AntiVirus Produkten der unterschiedlichen Hersteller, inklusive Symantec, F-secure, Trend Micro, McAfee, Computer Associates, ClamAV und Sophos entdeckt. Diese Schwachstellen können dazu verwendet werden, um mit wenig oder gar keiner User Interaktion die totale Kontrolle über die Systeme zu erlangen.

AntiVirus Software ist auch gegen so genannte "evasion" Attacken anfällig. Mit speziell geschriebenen böartigen Dateien, z.B. eine HTML Datei mit einem exe Header kann AntiVirus scanning umgehen. Die evasion Attacke kann dazu verwendet werden, um die Vireninfectionsrate zu erhöhen.

C2.2 Betroffene Betriebssysteme

Jedes System, dass eine AntiVirus Software oder eine Virenerkennungseingine verwendet, kann davon betroffen sein. Das inkludiert Installationen auf Desktops, Servern und Gateways. Jede Plattform kann betroffen sein, inklusive aller Microsoft Windows und Unix Systeme.

C2.3 CVE Einträge

AhnLab
[CVE-2005-3029](#), [CVE-2005-3030](#)

Avast!
[CVE-2005-2384](#), [CVE-2005-2385](#)

AVIRA
[CVE-2005-2957](#)

BitDefender
[CVE-2005-3154](#)

ClamAV
[CVE-2005-2450](#), [CVE-2005-2920](#)

Computer Associates
[CVE-2005-1693](#)

HAURI
[CVE-2004-2720](#), [CVE-2005-2670](#), [CVE-2005-2041](#)

F-Secure
[CVE-2004-2405](#), [CVE-2005-2937](#), [CVE-2005-0350](#)

Kaspersky
[CVE-2005-2937](#), [CVE-2005-3142](#)

McAfee
[CVE-2005-0643](#), [CVE-2005-0644](#)

Sophos
[CVE-2005-2768](#)

Symantec
[CVE-2005-0249](#)

Trend Micro
[CVE-2005-0533](#)

ZoneAlarm
[CVE-2005-1693](#)

C2.4 Wie erkennt, ob man gefährdet ist

Wenn Sie AntiVirus Software verwenden, die nicht auf dem letzten Stand ist, sind Sie wahrscheinlich betroffen.

C2.5 Wie man sich gegen diese AntiVirus Schwachstellen schützt

- Stellen Sie sicher, dass alle AntiVirus Software regelmäßig und automatisch aktualisiert wird.
- Überprüfen Sie regelmäßig die Webseite des Herstellers für Upgrades, Patches und Security Advisories. Eine Liste von AntiVirus Herstellern ist in der weiterführenden Hinweisen zu finden. Bitte beachten Sie, dass diese Liste nicht vollständig sein kann.

- Wenn Sie AntiVirus Software auf Gateways und Desktops installiert haben, wird empfohlen, AntiVirus Lösungen von unterschiedlichen Herstellern zu verwenden. Wenn eine Schwachstelle in einer AntiVirus Software entdeckt wird, ergibt das keinen "single point of failure".

C2.6 Weiterführende Informationen

Nachfolgend ist eine Liste von AntiVirus Herstellern, um nach Upgrades, Patches und Security Advisories zu suchen.

Anti-virus Security Advisories

- <http://www.sans.org/newsletters/risk/display.php?v=4&i=6> (Symantec)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=6> (F-Secure)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=8#widely2> (Trend Micro)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=12#widely1> (McAfee)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=21#widely1> (Computer Associates)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=30#widely1> (ClamAV)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=38> (ClamAV)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=34#other2> (HAURI)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=35#widely2> (Sophos)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=38#other2> (AhnLab and AVIRA)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=42#other4> (AhnLab)
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=40#other3> (Kaspersky)

Anti-virus Evasion Issues

- <http://www.kb.cert.org/vuls/id/968818>
- <http://www.uniras.gov.uk/vuls/2004/380375/mime.htm>
- <http://www.sans.org/newsletters/risk/display.php?v=4&i=43#other4>

Andere Anti-virus Resources

- http://www.cert.org/other_sources/viruses.html
- <http://www.virusbtn.com/>
- <http://www.eicar.com/>
- <http://www.wildlist.org/>

C3. PHP-based Anwendungen

C3.1 Beschreibung

PHP ist die am weitesten verbreitete Scripting Language für da Web. Gemäß einiger Reports haben 50% der Apache Server weltweit PHP installiert. Eine große Anzahl von Content Management Systemen (CMS), Portale, Bulletin Boards, Diskussions Foren sind in PHP geschrieben. Im letzten Jahr gab es keine Woche, in der nicht ein Problem in einer Software die PHP verwendet, entdeckt wurde. Die typischen Schwachstellen, die während des letzten Jahres entdeckt wurden sind:

- Schwachstelle im PHP Packet. Exploit Code ist für einige Schwachstellen verfügbar.
- Remote File inkludiert Schwachstelle in der Anwendung mit PHP. Diese sind üblich und leicht auszunutzen. Dieser Fehler ermöglicht einen Angreifer beliebigen Code auf den betroffenen Web Server auszuführen.
- Remote Command Execution Schwachstelle in der Anwendung mit PHP. Diese sind leicht auszunutzen und die Erkenntnis wird üblicherweise im Internet als ein proof of concept code veröffentlicht. [Santy Wurm](#) resultiert aus so einer Schwachstellein dem populären Bulletin Board- phpBB.
- SQL Injection Schwachstelle in der Anwendung mit PHP. Diese sind leicht auszunutzen und werden genutzt um Kennwort Hashes für die Administratoren der PHP Anwendung zu entfernen.
- Remote Code Execution Schwachstelle in Libraries beinhaltet in PHP. Zum Beispiel PHP XML-RPC und Pear XML-RPC Libraries werden von einer Anzahl von Software Projekten verwendet. [Lupper Wurm](#) nützt Remote Code Execution Schwachstellen in diesen Libraries aus.

Die letzten drei Arten von Schwachstellen resultieren aus einem nicht erfolgten Löschen von Daten auf temporären Speichermedien von Anwendereingaben. Die Verfügbarkeit von Web Scanning Tools hat den Prozess, diese Schwachstellen zu finden automatisiert.

C3.2 Betroffene Software

Web Server, die nicht die letztgültige Version des PHP Pakete verwenden. Wenn Sie ältere PHP Software verwenden, sind Sie höchst wahrscheinlich gefährdet.

C3.3 CVE Einträge

[CVE-2004-0594](#), [CVE-2005-3389](#), [CVE-2005-3390](#)

Hinweis: Es gibt nicht viele CVE Einträge für PHP-basierenden Anwendungen.

C3.4 Wie erkennt, ob man gefährdet ist

Scannen Sie die Web Server periodisch mit [Vulnerability Scanners](#). Das ist die beste Methode, da die Anzahl von Schwachstellen in PHP Anwendungen jede Woche steigt und es schwer wird, den Überblick zu behalten, speziell wenn Sie mehrere PHP Anwendungen auf Ihren Servern ausführen.

C3.5 Wie man sich gegen diese PHP Schwachstellen schützt

- Installieren Sie alle Hersteller Patches für PHP und PHP-basierenden Anwendungen.
- Häufiges Web scannen ist empfohlen wenn eine große Anzahl von PHP Anwendungen verwendet werden.
- Verwenden Sie die folgende sichere PHP Konfiguration:
 - `register_globals` (sollte off sein)
 - `allow_url_fopen` (sollte off sein)
 - `magic_gpc_quotes` (sollte off sein für gut geschriebene Software, sollte on sein für schlecht geschriebene PHP 3 und PHP 4 Scripts)
 - `safe_mode` and `open_basedir` (sollte enabled und richtig konfiguriert sein)
- Konfigurieren Sie Apache `mod_security` und `mod_rewrite` Filter um PHP Attacken zu blockieren.
- Verwenden Sie Programme wie [Paros Proxy](#), um automatisierte SQL Injection Tests gegen Ihre PHP Anwendungen durchzuführen.
- Upgraden Sie zu PHP 5, da es viele latente PHP Sicherheitsprobleme behebt.
- Folgen Sie den "Least Privilege" Prinzip, um PHP Programme wie PHPsuExec, php_suexec oder suPHP von [suPHP](#) auszuführen.
- Verwenden Sie [Intrusion Prevention/Detection Systeme](#) um bösartige HTTP Requests zu blockieren.

C3.6 Weiterführende Informationen

PHP Schwachstellen

http://www.hardened-php.net/advisory_202005.79.html

http://www.hardened-php.net/advisory_152005.67.html

http://www.hardened-php.net/advisory_142005.66.html

<http://www.sans.org/newsletters/risk/display.php?v=3&i=50#widely4> <http://www.sans.org/newsletters/risk/display.php?v=3&i=23#other1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=28#widely4>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=48#exploit1>

Hardened PHP Project

<http://www.hardened-php.net>

OWASP Webpage (Beinhaltet Programme und Dokumente zum Testen von Schwachstellen in Web Anwendungen)

<http://www.owasp.org>

PHP Security Features

<http://au.php.net/features.safe-mode>

C4. Datenbank Software

C4.1 Beschreibung

Datenbanken sind das Schlüsselement vieler Systeme, die große Mengen von Daten speichern, suchen oder manipulieren. Sie werden in allen Geschäfts-, Finanz-, Banken-, Kundenbeziehungs- und Systemüberwachungsanwendungen verwendet.

Durch die wichtigen gespeicherten Informationen wie Personen- und Finanzdaten sind Datenbanken oft Ziel von Angriffen. Da Datenbanken sehr komplexe Anwendungen sind und üblicherweise aus einer Anzahl von Programmen besteht, ergeben sich eine Vielzahl von Angriffsmöglichkeiten. Die am weitesten verbreiteten Datenbankschwachstellen, die heutzutage gefunden werden, können in folgender Weise klassifiziert werden:

- Buffer Overflows in Prozessen, die auf bekannte TCP/UDP Ports hören
- SQL Injection via dem Web Front End der Datenbank
- Datenbanken, die in standardmäßigen Konfigurationen mit standardmäßigen User und Kennwörtern betrieben werden
- Datenbanken mit schlechten Kennwörtern auf privilegierten Accounts

Es sind viele verschiedene Datenbanksysteme verfügbar. Einige der bekanntesten sind Microsoft SQL Server (proprietär, läuft unter Windows), Oracle (proprietär, läuft auf vielen Plattformen), IBM DB2 (proprietär, läuft auf vielen Plattformen), MySQL und PostgreSQL (beide Open Source und verfügbar für viele Plattformen).

Alle modernen relationalen Datenbanksystemen sind Port adressierbar, dass jeder mit fertig verfügbaren Tools versuchen kann, eine Verbindung zur Datenbank herzustellen. Dabei werden Sicherheitsvorkehrungen des Betriebssystems umgangen. Zum Beispiel Microsoft SQL Server können über TCP Port 1433, Oracle über TCP Port 1521, IBM DB2 über Ports 523 und 50000 und höher, MySQL über TCP Port 3306 und PostgreSQL über TCP Port 5432 erreicht werden.

Während des letzten Jahres hat Oracle kumulative Updates veröffentlicht, die hunderte Schwachstellen beheben. Obwohl nicht alle Schwachstellen als kritisch einzustufen sind, sind die Administratoren gezwungen diese Updates zu installieren, um die kritischen Probleme zu beheben.

Funktionierende Exploits sind für viele Datenbanken im Internet verfügbar.

C4.2 Betroffene Betriebssysteme

Open Source Datenbanken sind auf allen üblichen Betriebssystemen verfügbar. Viele kommerzielle DBMS laufen ebenfalls auf verschiedenen Plattformen

C4.3 CVE Einträge

Dies sind die Einträge seit Juli 2004. Frühere Schwachstellen können in früheren Versionen der Top 20 Schwachstellen gefunden werden.

Oracle

[CVE-2004-0637](#), [CVE-2004-0638](#), [CVE-2004-1338](#), [CVE-2004-1363](#), [CVE-2004-1364](#), [CVE-2004-1365](#), [CVE-2004-1366](#), [CVE-2004-1369](#), [CVE-2004-1370](#), [CVE-2004-1371](#), [CVE-2005-1495](#), [CVE-2004-1774](#)

Hinweis: Alle CVEs von den kumulativen Patches von Oracle sind hier nicht aufgeführt.

MySQL

[CVE-2004-0627](#), [CVE-2004-0628](#), [CVE-2004-0836](#), [CVE-2005-0684](#), [CVE-2005-1274](#), [CVE-2005-2558](#)

PostgreSQL

[CVE-2005-0244](#), [CVE-2005-0247](#)

IBM DB2

[CVE-2004-0795](#), [CVE-2004-1372](#)

C4.4 Wie erkennt, ob man gefährdet ist

Da Datenbanken oft als Komponenten in anderen Anwendungen verteilt sind, ist es möglich, dass eine Datenbank installiert wurde, ohne dass es der Administrator weiß. Datenbanken können daher ungepatcht bleiben oder in standardmäßigen unsicheren Konfigurationen auf den Systemen vorhanden sein. Es ist nicht ausreichend, eine einfache Liste der installierten Anwendungen zu kontrollieren! Das wurde am besten demonstriert mit dem SQL Slammer Wurm, der die Microsoft Data Access Component (MDAC) ausnutzte, welche in vielen Anwendungen inkludiert ist.

Führen Sie eine Schwachstellenüberprüfung auf den Systemen durch um festzustellen, welche DBMS Software verfügbar, erreichbar und anfällig ist. Sie können jeden [Vulnerability Scanner](#) oder Tools von Datenbankherstellern wie [MySQL Network Scanner](#), Microsoft [SQL server tool](#) verwenden.

C4.5 Wie man sich gegen diese Datenbank Schwachstellen schützt

- Stellen Sie sicher, dass alle DBMS gepatcht und aktuell sind. Ungepatchte oder veraltete Versionen sind höchst wahrscheinlich anfällig. Überprüfen Sie die Hersteller Sites für Patch Informationen. Bleiben Sie auf dem aktuellen Stand der Schwachstellen, die von den Herstellern veröffentlicht werden:
 - Oracle Security Alerts (<http://otn.oracle.com/deploy/security/alerts.htm>)
 - MySQL (<http://lists.mysql.com/>)
 - PostgreSQL (<http://www.postgresql.org/community/>)
 - Microsoft SQL (<http://www.microsoft.com/technet/security/bulletin/notify.msp>)
 - IBM DB2 (<http://www-306.ibm.com/software/data/db2/udb/support/>)
- Stellen Sie sicher, dass die DBMS und die Anwendungen sicher konfiguriert wurden:
 - Verwenden Sie minimale Privilegien.
 - Entfernen/Ändern Sie Standardkennwörter auf den Datenbank Accounts und den System Accounts, bevor die Systeme in das Netz ausgerollt werden.
 - Verwenden Sie Stored Procedures wo möglich.
 - Entfernen/Ändern Sie unnötige Stored Procedures.
 - Setzen Sie Längenlimits für Formfelder.

Es gibt einige sehr brauchbare Quellen, die dabei helfen können, um DBMS sicher zu machen, wie in dem Abschnitt für weiterführende Hinweise zu lesen ist.

- Verwenden Sie Firewalls oder andere Netzwerksicherheitseinrichtungen um Netzwerkzugang zu den Ports der Datenbanken führen, einzuschränken.
- Vertrauen Sie nie dem User Input! Stellen Sie sicher, dass die Anwendungen, die zu den Datenbanken verbunden sind, alle Anwendereingaben löschen, um nicht für Angriffe wie SQL Injection (siehe <http://www.sans.org/rr/whitepapers/securecode/23.php>) anfällig zu sein.

C4.6 Weiterführende Informationen

SANS Reading Room über Database Security
http://www.sans.org/rr/catindex.php?cat_id=3

Oracle
SANS Comprehensive Security Checklist für Oracle
<http://www.sans.org/score/oraclechecklist.php>
https://store.sans.org/store_item.php?item=80

CIS Oracle Benchmark Tool
http://www.cisecurity.org/bench_oracle.html

Oracle Security Information kann gefunden werden unter
<http://www.petefinnigan.com/orasec.htm>
<http://otn.oracle.com/deploy/security/index.html>

MySQL
SecurityFocus step-by-step Guide um MySQL sicher zu machen
<http://www.securityfocus.com/infocus/1726>

MySQL Security
<http://dev.mysql.com/doc/mysql/en/Security.html>

PostgreSQL Security Guide
<http://www.postgresql.org/docs/7/interactive/security.html>

Microsoft SQL Security Guide
<http://www.microsoft.com/sql/techinfo/administration/2000/security/default.mspx>

IBM DB2
http://www.net-security.org/dl/articles/Securing_IBM_DB2.pdf

C5. File Sharing Anwendungen

C5.1 Beschreibung

Eine rasch anwachsende Gruppe von Anwendern verwendet Peer-to-Peer File Sharing Programme (P2P). Diese Anwendungen werden zum Herunterladen und Verteilen von Daten wie Musik, Video, Bildern, Texten, Source Code, usw. verwendet. P2P Anwendungen werden außerdem legitim für die Verteilung von übersetzter Open Source/GPL Software und ISO Images von bootfähigen Linux Distributionen eingesetzt. Allerdings sind diese Daten oft von fragwürdiger Natur oder urheberrechtlich geschützt.

P2P Programme arbeiten über ein verteiltes Netzwerk von Clients, die Verzeichnisse mit Dateien oder ganze Festplatten mit Daten freigeben. Clients nehmen daran teil, indem sie Dateien von anderen Usern herunterladen, ihre Daten anderen zur Verfügung stellen und Dateisuchen für andere koordinieren.

Die meisten der P2P Programme verwenden eine Liste von Standardports, aber sie können automatisch oder manuell so umkonfiguriert werden, dass sie andere Ports verwenden um nicht entdeckt zu werden oder Firewalls oder Ausgangsfilter zu umgehen. Der Trend scheint sich auf die Verwendung von http Wrappern und Verschlüsselung hin zu bewegen um so leicht interne Vorschriften und Einschränkungen zu umgehen.

Die hauptsächlichen Bedrohungen, die von P2P Anwendungen ausgehen, sind:

- Von der Ferne ausnutzbare Schwachstellen in P2P Anwendungen durch die P2P Clients oder Server beeinträchtigt werden können.
- Viren und Bots verwenden freigegebene P2P Ordner für ihre Verbreitung indem sie bösartige Dateien mit verlockenden Namen in diese Ordner kopieren.
- P2P Software ist normalerweise mit Spyware und Adware gebündelt. Das verschlimmert die Infektion mit Spyware/Adware in einer Organisation.
- Angreifer können bösartige Dateien als legitime Musik- oder Videodateien tarnen. Wenn Anwender diese Dateien herunterladen, kann deren System infiziert und als "Bot" verwendet werden.
- P2P Freigaben haben üblicherweise kein oder nur ein schwaches Passwort. Dies kann leicht ausgenutzt werden um eine Freigabe mit bösartigen Dateien zu infizieren.
- Eine Organisation kann für Urheberrechtsverletzungen haftbar gemacht werden.
- P2P-Verkehr kann wesentlich zur Nutzung der Bandbreite beitragen und so andere kritische Anwendungen verlangsamen. Das kann besonders die Qualität von Sprach- und Videodatenverkehr in einer Organisation beeinträchtigen.

Für einige der Buffer Overflow Schwachstellen in P2P Software existiert Exploit Code. Laut den Forschungen von Symantec, haben in der zweiten Hälfte von 2004 6% der Attacken aus dem Internet versucht Schwachstellen in eDonkey auszunutzen, weitere 5% versuchten das in Gnutella.

Die Zahl der Bedrohungen durch die Verwendung von P2P, IM, IRC und CIFS unter den "Top 50 malicious code" von Symantec ist im vergangenen 6-Monate-Beobachtungszeitraumum 39% angestiegen.

C5.2 Betroffene Betriebssysteme

P2P Software existiert für alle derzeit verwendeten Windows Betriebssysteme, wie auch für Linux, UNIX und MacOS Systeme.

C5.3 CVE Einträge

[CVE-2004-1114](#), [CVE-2004-1286](#), [CVE-2004-1892](#), [CVE-2004-2433](#), [CVE-2005-0595](#), [CVE-2005-1806](#)

C5.4 Wie erkennt, ob man gefährdet ist

P2P Aktivitäten im Netzwerk zu erkennen kann sich als schwierig herausstellen.

- Man kann im Netzwerk verwendete P2P Software entdecken, in dem man den Datenverkehr beobachtet und nach bestimmten Ports oder bestimmten Strings der Anwendungsschicht, die häufig von P2P Software verwendet werden, durchsucht. Am Ende dieses Kapitels befindet sich eine Liste mit häufig von P2P Software verwendeten Ports.
- Es gibt eine Reihe von Anwendungen und Diensten, die bei der Erkennung oder Verhinderung von P2P-Verkehr unterstützen. Manche hostbasierte Intrusion Prevention Systeme können die Installation oder die Ausführung von P2P Anwendungen verhindern.
- Netzwerkbasierte Intrusion Detection/Prevention Systeme können P2P-Verkehr entdecken, ihn am "Betreten beziehungsweise Verlassen" des Netzwerk hindern oder den Verkehr beobachten.
- Beobachtung der WAN-Verbindungen mit Anwendungen wie NTOP kann auch P2P-Verkehr enthüllen.
- Man könnte auch Speicherbereiche im Netzwerk nach Inhalten, die üblicherweise von Anwendern heruntergeladen werden, wie zum Beispiel *.mp3, *.wma, *.avi, *.mpg, *.mpeg, *.jpg, *.gif, *.zip, *.torrent oder *.exe, durchsuchen.
- Die Überwachen von Datenträgern nach plötzlicher Abnahme des freien Speichers kann auch nützlich sein.
- Scanner verfügen oft über ein Plugin um laufende P2P Anwendungen zu entdecken, und für Rechner mit Microsoft Windows kann SMS verwendet werden um herauszufinden welche Programme auf den Workstations installiert sind.

C5.5 Wie man sich vor Schwachstellen in P2P Software schützen kann

- Normale Anwender sollte es nicht erlaubt werden, Software, insbesondere Peer-to-Peer-Software, zu installieren. Um normale Anwender an der Installation von nicht genehmigter Software zu hindern, wird empfohlen diesen Usern keine Administratorrechte zu geben. Um die unbeabsichtigte Installation von nicht genehmigter Software durch Benutzer mit Administratorrechten zu verhindern, können Tools wie [DropMyRights](#) von Microsoft verwendet werden um beliebige Webbrowser oder Mail Clients abzusichern. In Active Directory Umgebungen können Software Restriction Group Policies verwendet werden um zu verhindern daß bekannte Typen von Binaries ausgeführt werden..
- Ausgangsfilter sollten den Zugriff auf Ports, die nicht für Geschäftszwecke benötigt werden, einschränken. Allerdings wird das immer weniger effektiv, da immer mehr P2P Anwendungen http verwenden.
- Kontrollieren Sie Ihr Netzwerk auf P2P-Verkehr und adressieren Sie Verletzungen der Richtlinien durch geeignete Kanäle. Das kann durch Überwachung von Firewalls und IDS Logs erreicht werden. Es gibt auch Lösungen für Firmen, die nicht genehmigte P2P- und IM-Verbindungen entdecken und blockieren.
- Man kann auf einzelnen Workstations mit Tools wie Microsoft PortQry oder Port Reporter ungewöhnliche Netzwerkaktivitäten überwachen und loggen.
- Verwenden Sie unternehmensweit Antivirus- und Antispywareprodukte und stellen Sie sicher, daß täglich Aktualisierungen durchgeführt werden.
- Verwenden Sie zusätzlich zu den Netzwerkfirewalls auch hostbasierte Firewalls. Windows XP und Windows 2003 enthalten die Windows Firewall, die, wenn sie richtig konfiguriert wurde, adäquaten Schutz bietet. Weitere Third-Party hostbasierte Firewalls (ZoneAlarm, Sygate, Outpost) stellen weitere Fähigkeiten und Flexibilität zur Verfügung. Windows 2000, XP und 2003 Systems können auch IPSec Policies verwenden um anhand der verwendeten Ports unnötigen Netzwerkverkehr zu filtern. In Active Directory Umgebungen können IPSec Policies und die Konfiguration der Windows Firewall (für Windows XP2 und Windows 2003 SP1) auch zentral durch Group Policies verwaltet werden.
- Deaktivieren Sie die "Einfache Dateifreigabe" von Windows XP, wenn sie nicht unbedingt benötigt wird. Start - Einstellungen - Systemsteuerung - Ordneroptionen - Ansicht - "Einfache Dateifreigabe verwenden" deaktivieren (Häkchen entfernen) - OK.
- Kontrollieren Sie die Systeme auf die Anwesenheit unbekannter ausführbarer Dateien und die nicht erlaubte Veränderung von Systemdateien. Softwareprodukte wie Tripwire (von diesem Produkt gibt es kommerzielle und Open Source-Versionen) können verwendet werden um Änderungen in Dateien zu erkennen.

Gewöhnlich von Peer-to-Peer Anwendungen verwendete Protokolle und Ports

P2P Dienst	Standard/primärer Port oder Port-Bereich, TCP	Standard/primärer Port oder Port-Bereich, UDP
BearShare	6346	
Bittorrent	2181, 6881-6999	
Blubster		41170-41350
eDonkey	4661-4662	5737
eDonkey2000	4661-4662	4665
eMule	4661-4662,4711	4665,4672
Gnutella	6346/6347	6346/6347

Groupier	8038	8038
Kazaa	1214	1214
Limewire	6346/6347	6346/6347
Morpheus	6346/6347	6346/6347
Shareaza	6346	6346
WinMx	6699	6257

C5.6 Weiterführende Informationen

US DHS Information Bulletin "Unauthorized Peer-to-Peer (P2P) Programs on Government Computers"

http://www.dhs.gov/interweb/assetlibrary/IAIP_UnauthorizedP2PProgramsGovtComp_041905.pdf

Federal Law Enforcement Announces Operation D-Elite, Crackdown on P2P Piracy Network: First Criminal Enforcement Against BitTorrent Network Users

<http://www.usdoj.gov/criminal/cybercrime/BitTorrent.htm>

Cyber Security Tip ST05-007 - Risks of File-Sharing Technology

<http://www.us-cert.gov/cas/tips/ST05-007.html>

Risks of P2P File Sharing

<http://www.ftc.gov/bcp/workshops/filessharing/presentations/hale.pdf>

Symantec Internet Security Threat Report - Trends for July 04- December 04

Volume VII, Published March 2005

<http://ses.symantec.com/pdf/ThreatReportVII.pdf>

Securing Windows XP Professional in a Peer-to-Peer Networking Environment

http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/sec_winxp_pro_p2p.mspix

Identifying P2P users using traffic analysis - Yiming Gong - 2005-07-21

<http://www.securityfocus.com/infocus/1843>

Sinit P2P Trojan Analysis

<http://www.lurhq.com/sinit.html>

How to block specific network protocols and ports by using IPSec (MS KB article 813878)

<http://support.microsoft.com/kb/813878>

Using Software Restriction Policies to Protect Against Unauthorized Software

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspix>

Availability and description of the Port Reporter tool (MS KB article 837243)

<http://support.microsoft.com/kb/837243>

New features and functionality in PortQry version 2.0 (MS KB article 832919)

<http://support.microsoft.com/default.aspx?kbid=832919>

Log Parser 2.2

<http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspix>

Browsing the Web and Reading E-mail Safely as an Administrator (DropMyRights)

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp>

Peer-to-Peer (P2P) Security and QoS Frequently Asked Questions (CheckPoint)

http://secureknowledge.checkpoint.com/pub/sk/docs/public/firewall1/ng/pdf/p2p_faq.pdf

C6. DNS Software

C6.1 Beschreibung

Das Domain Name System (DNS) ist ein wesentlicher Internet-Mechanismus der vor allem die Übersetzung von weltweit eindeutigen Rechnernamen in ebenso weltweit eindeutige Internet Protocol Adressen durch ein Schema verteilter Datenbanken ermöglicht. Dabei stützt sich DNS auf ein Vertrauensmodell, das in einer Ära gegenseitigen Vertrauens, die sich sehr vom heutigen im Allgemeinen feindseligen Internet unterscheidet, entwickelt wurde. Aufgrund dieser Änderung in der Art des Internet ist DNS für vielen Attacken in Transaktionen anfällig, die dieses Vertrauen ausnützen. Unter diesen Attacken sind Cache Poisoning, Domain Hijacking und Man-in-the-middle Redirection. Während des vergangenen Jahres wurden Cache Poisoning-Schwachstellen verwendet um Anwender zu böswilligen Domains umzuleiten um Malware auf den Systemen der Benutzer zu installieren. Offene rekursive DNS Server werden aktiv als DDoS Reflektoren verwendet, wodurch sich ein enormer Verstärkungsfaktor erreichen lässt.

C6.2 Betroffene Software

Symantec Gateway Security

Symantec Enterprise Firewall

Symantec VelociRaptor

DNSmasq DNS Server

Windows NT und Windows 2000 (vor SP3) DNS Servers mit Standardkonfiguration

Windows DNS Server, die Requests an BIND DNS Server mit den Versionen 4.x oder 8.x weiterleiten

Windows DNS Server, die Requests an andere verwundbare Windows DNS Server weiterleiten

C6.3 CVE Einträge

[CVE-2005-0817](#), [CVE-2005-0877](#)

C6.4 Wie erkennt, ob man gefährdet ist

Alle Internet-Anwender sind dem Risiko, fehlerhafte Daten von DNS Servern zu erhalten, ausgesetzt. Wenn das Scannen der DNS Server in Ihrem Einflussbereich zeigt, daß weder die aktuellen Versionen oder Patches, die vom Hersteller der DNS Software veröffentlicht wurden, installiert sind, dann ist/sind diese DNS Server gefährdet.

Ein proaktiver Ansatz um die Sicherheit von DNS Servern zu erhalten ist, angepasste Berichte und Alarmer, wie unter anderem von SANS oder Secunia verfügbar, zu abonnieren oder die bei der Open Source Vulnerability Database (<http://www.osvdb.org>) veröffentlichten Hinweise regelmäßig zu lesen. Zusätzlich zu den Sicherheitswarnungen kann auch ein aktualisierter Schwachstellenscanner sehr effektiv sein um potentielle Schwachstellen von DNS Servern zu erkennen.

C6.5 Wie man sich vor DNS Schwachstellen schützen kann

Wie bei jedem Softwarepaket müssen Updates und Patches für DNS Server-Software sofort bei Verfügbarkeit und unmittelbar nachdem deren Auswirkungen auf den Betrieb des lokalen Netzwerks getestet wurden eingespielt werden.

Allgemeine Schützmaßnahmen gegen DNS Schwachstellen:

- Installation aller Patches vom Hersteller oder Upgrade der DNS Server auf die neueste Version. Weitere Informationen über das Härten einer DNS Installation gibt es in den Artikeln über die Absicherung von Namensdiensten, die in der Unix Security Checklist des CERT angeführt sind.
- Installation geeigneter Firewallregeln für alle DNS Server innerhalb des Netzwerks, auf die kein direkter Zugriff aus dem Internet erfolgen muss.
- Um die Zonentransfers zwischen primären und sekundären DNS Servern kryptographisch abzusichern, konfiguriert man die Server so, daß sie das DNS Transaction Signatures (TSIG) verwenden.
- Gefängnis: um unter Unix zu verhindern, daß ein beeinträchtigter DNS Dienst das ganze System entblößt, schränkt man den Dienst so ein, daß er als nichtprivilegiertes Benutzer in einem `gechroot()` Verzeichnis läuft.
- Verbieten Sie die Verwendung Ihrer rekursiven DNS Server für alle außer Ihrem eigenen Netzwerk außer es wird benötigt. Firewalls oder die Konfiguration des DNS können dies in den meisten Fällen verhindern. Die Deaktivierung von Rekursion und Glue Fetching helfen, den DNS Cache vor DNS Cache Poisoning zu schützen.
- Erwägen Sie Ihre gesamte Zone zu signieren, indem Sie die DNS Security Extensions (DNSSEC) verwenden.
- Auf den meisten Systemen, die BIND verwenden, zeigt der Befehl "`named -v`" die installierte Version, dargestellt als X.Y.Z, wobei X die Hauptversion ist, Y die Unterversion und Z der Patchlevel. Die beiden aktuellen Hauptversionen von BIND sind 8 und 9. Das Internet Systems Consortium empfiehlt allen BIND Anwendern, so rasch wie möglich auf Version 9 umzusteigen.
- DNS Server sind in viele weitverbreitete Produkte wie Firewalls, Netzwerkservers für Unternehmen und Sicherheitsappliances integriert. Bei allen Server, Appliances und Systeme, die das Internet verwenden, muss sichergestellt werden, dass eingebaute DNS Software aktualisiert und gemäß den Empfehlungen des Herstellers gewartet ist.
- Auf Servern, die nicht dafür gedacht sind, DNS-Transaktionen zu unterstützen (zum Beispiel Mail-, Web- oder Dateiserver), sollten kein DNS Server als Anwendung oder Dämon laufen, außer es ist unbedingt erforderlich.

C6.6 Weiterführende Informationen

DNS Schwachstellen

<http://www.sans.org/newsletters/risk/display.php?v=4&i=11>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=14#widely1>

<http://iscsans.org/presentations/dnspoisoning.php>

<http://thekelleys.org.uk/dnsmasq/doc.html>

<http://www.icir.org/vern/papers/reflectors.CCR.01/node8.html>

Erfassung der DNS Versionen und der DNS Server Software

<http://mydns.bboy.net/survey/>

<http://www.dns.net/dnsrd/servers/>

Interne Abläufe im DNS

<http://www.internic.net/faqs/authoritative-dns.html>

<http://www.sans.org/rr/whitepapers/dns/>

<http://www.cert.org/archive/pdf/dns.pdf>

<http://www.isc.org/index.pl>

<http://www.microsoft.com/windows2000/technologies/communications/dns/default.msp>

<http://www.dns.net/dnsrd/>

Einsatz von DNSSEC

<http://www.dnssec-deployment.org/>
<http://www.dnssec.net>
<http://csrc.nist.gov/publications/drafts/DRAFT-SP800-81.pdf>

DNS Security Best Practices

<http://www.cymru.com/Documents/secure-bind-template.html>
<http://www.softpanorama.org/DNS/security.shtml>
http://cookbook.linuxsecurity.com/sp/bind_hardening8.html
<http://www.isc.org/index.pl?sw/bind/bind-security.php>

C7. Mediaplayer

C7.1 Beschreibung

Mediaplayer sind sehr populär und sind auf Millionen von Systemen installiert. Die steigende Anzahl von Breitbandverbindungen hat ermöglicht, dass mehr Inhalte in der Form von Multimediadateien wie Filme, Videos oder Musik heruntergeladen werden. Diese Inhalte werden in Webseiten oder Präsentationen eingebaut oder in Multimediaanwendungen integriert.

Mediaplayer finden Ihren Weg auf Systeme durch Standardinstallation oder sie kommen gebündelt mit anderer Software. Üblicherweise werden Browser so konfiguriert, daß man "bequem" Mediendateien ohne weiteres Zutun des Benutzers herunterladen und öffnen kann.

Zahlreiche Schwachstellen in verschiedenen Mediaplayern wurden im letzten Jahr entdeckt. Viele dieser Schwachstellen erlauben böswilligen Webseiten oder Mediendateien Computer wesentlich zu beschädigen ohne Eingriffe der Anwender. Das System des Anwenders kann ganz einfach durch Besuch einer böswilligen Webseite beeinträchtigt werden. Daher können diese Schwachstellen benutzt werden um böswillige Software wie Spyware, Trojaner, Adware oder Keylogger auf den Systemen der Benutzer zu installieren. In vielen Fällen ist der dazu benötigte Code öffentlich verfügbar.

Einige der populäreren Mediaplayer sind:

Windows: Windows Media Player, RealPlayer, Apple Quicktime, Winamp, iTunes

Mac OS: RealPlayer, Quicktime, iTunes

Linux/Unix: RealPlayer, Helix Player

C7.2 Betroffene Betriebssysteme

Microsoft Windows, Unix/Linux und Apple Mac OS X

C7.3 CVE Einträge

RealPlayer and Helix Player

[CVE-2004-0550](#), [CVE-2004-1094](#), [CVE-2004-1481](#), [CVE-2005-0189](#), [CVE-2005-0191](#), [CVE-2005-0455](#), [CVE-2005-0611](#), [CVE-2005-0755](#), [CVE-2005-1766](#), [CVE-2005-2052](#), [CVE-2005-2054](#), [CVE-2005-2055](#), [CVE-2005-2710](#), [CVE-2005-2055](#)

iTunes

[CVE-2005-0043](#), [CVE-2005-1248](#)

Winamp

[CVE-2004-0820](#), [CVE-2004-1119](#), [CVE-2004-1150](#), [CVE-2004-1896](#), [CVE-2005-2310](#)

Quicktime

[CVE-2004-0431](#), [CVE-2004-0926](#), [CVE-2005-2743](#), [CVE-2005-2753](#), [CVE-2005-2754](#)

Windows Media Player

[CVE-2004-1244](#), [CVE-2004-1324](#)

Macromedia Flash Player

[CVE-2005-2628](#)

C7.4 Wie erkennt, ob man gefährdet ist

Wenn Sie einen dieser Player verwenden, aber nicht die neueste Version mit allen verfügbaren Patches verwenden, dann sind Sie für die damit verbundenen Attacken anfällig. Regelmäßige Kontrolle der installierten Software kann verwendet werden um unbeabsichtigte Installationen von Mediaplayern zu entdecken.

C7.5 Wie man sich vor diesen Schwachstellen schützen kann

Folgende Ansätze werden verfolgt um sich vor diesen Schwachstellen zu schützen:

- Halten Sie Mediaplayer mit den neuesten Patches aktuell. Die meisten Player ermöglichen Updates über das Hilfe- oder Extras-Menü.
- Überprüfen Sie gründlich die Standardinstallationen von Betriebssystemen und anderen Produkten um sicherzustellen, dass sie keine unerwünschten Mediaplayer enthalten. Konfigurieren Sie das Betriebssystem und Browser so, dass unbeabsichtigte Installationen verhindert werden.
- Verwenden Sie [Intrusion Prevention/Detection Systeme](#) und [Antivirus- und Malwareerkennungssoftware](#) um bösartige Mediendateien zu blockieren.

C7.6 Weiterführende Informationen

RealNetworks

Media Player Products Home Page

http://www.realnetworks.com/products/media_players.html

Sicherheitsberichte

<http://service.real.com/help/faq/security/>

http://service.real.com/help/faq/security/051110_player/EN/

<http://www.sans.org/newsletters/risk/display.php?v=4&i=40#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=25#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=16#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=10#exploit1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=9#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=43#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=39#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=23#widely4>

Helix Player

Home Page

<https://player.helixcommunity.org/>

News inklusive Sicherheitswarnungen

<https://helixcommunity.org/news/>

Apple

QuickTime Home Page

<http://www.apple.com/quicktime/>

iTunes Home Page

<http://www.apple.com/itunes/>

Apple Sicherheitsinformationen

<http://docs.info.apple.com/article.html?artnum=61798>

QuickTime Support

<http://www.apple.com/support/quicktime/>

Sicherheitsberichte

<http://www.sans.org/newsletters/risk/display.php?v=4&i=45#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=19#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=2#widely3>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=3#exploit1>

Nullsoft Winamp

Home Page

<http://www.winamp.com/>

<http://www.winamp.com/about/news.php>

Sicherheitsberichte

<http://www.sans.org/newsletters/risk/display.php?v=4&i=5#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=47#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=36#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=34#widely1>

Microsoft Windows Media Player

Home Page

<http://www.microsoft.com/windows/windowsmedia/default.aspx>

Windows Media Player 10 Sicherheit

<http://www.microsoft.com/windows/windowsmedia/mp10/security.aspx>

C8. Instant Messaging Anwendungen

C8.1 Beschreibung

Instant Messaging (IM) Anwendungen werden heute von Millionen von Anwendern für Privates und Geschäftliches verwendet. IM Anwendungen sind für nahezu alle Plattformen inklusive Handhelds verfügbar. Die heute populärsten IM Anwendungen sind: Yahoo! Messenger, AOL Instant Messenger, MSN Messenger, Jabber, Trillian, Skype und IRC. GoogleTalk wurde vor kurzem veröffentlicht und gewinnt an Marktanteilen. Von vielen dieser Anwendungen gibt es auch als Webversion für die ein Anwender keinen IM Client auf seinem System installieren muss. Diese Anwendungen stellen eine wachsende Bedrohung der Sicherheit für eine Organisation dar. Die Hauptbedrohungen sind Folgende:

- (a) Schwachstellen in IM Anwendungen können verwendet werden um ein System eines Anwenders zu kompromittieren. Während des letzten Jahres wurden Bufferoverflows im URI-Handler des AIM und in der Verarbeitung von PNG Bildern des MSN Messengers gefunden. Exploit Code ist für diese Schwachstellen verfügbar.
- (b) Die meisten dieser Anwendungen verfügen über die Fähigkeit, Dateien zu übertragen. Dieses Merkmal wird derzeit von vielen IM Würmern ausgenutzt um die Systeme von Benutzern mit Malware zu infizieren.
- (c) Der Transfer der Dateien kann auch zu Lecks von sensiblen Informationen führen.
- (d) Viele Würmer und Bots verwenden IRC Channels um mit dem Angreifer zu kommunizieren. Die IRC Channels können auch zum Starten von DDoS-Angriffen benutzt werden.
- (e) Einige dieser Anwendungen können Sprache übertragen, was zusätzlich zur Übertragung von Dateien zu unerwünschtem Verbrauch von Bandbreite führen kann.

C8.2 Betroffene Betriebssysteme

Instant Messaging Anwendungen sind für alle Plattformen inklusive Windows, UNIX und Mac OS.

C8.3 CVE Einträge

[CVE-2004-0597](#), [CVE-2004-0636](#), [CVE-2005-0243](#), [CVE-2005-0562](#), [CVE-2005-3265](#), [CVE-2005-3267](#)

C8.4 Wie man sich vor IM Schwachstellen schützen kann

- Richten Sie eine Firmenpolicy die die Verwendung von Instant Messaging innerhalb der Firma zu regeln. Kontrollieren Sie regelmäßig die Logs von Firewalls und Proxies um die Vorschriften der IM Verwendung zu forcieren.
- Schränken Sie die Möglichkeiten für Endbenutzer Software auf Clientworkstations zu installieren ein. Dies kann durch Entziehen der Administratorrechten auf Workstations erzielt werden.
- Stellen Sie sicher, daß jede installierte IM Anwendung wie Yahoo, MSN, AOL, Trillian, usw. mit den neuesten Patches aktualisiert ist.
- Konfigurieren Sie [Intrusion Prevention/Detection Systeme](#) so, dass Sie bei jeder Dateiübertragung mit einem Messagingprogramm einen Alarm erzeugt.
- Wenn es Ihre Securitypolicy erlaubt:
 - Blockieren Sie die folgenden Ports an der Firewall. Beachten Sie, dass das keinen kompletten Schutz bietet, da einige dieser Anwendungen Firewallregeln umgehen können.
 - 1503/tcp: MSN Messenger Application Sharing
 - 1863/tcp: Microsoft .NET Messenger, MSN Messenger
 - 4443/tcp: Yahoo Messenger File Sharing
 - 5050/tcp: Yahoo Messenger
 - 6891/tcp: MSN Messenger File Transfers
 - 5190-5193/tcp: AOL Instant Messenger
 - 13324-13325/tcp: MSN Messenger Audio und Video Conferencing
 - 5222-5223/tcp: Google Talk
 - 4000/udp - ICQ
 - Blockieren Sie den Zugriff auf Webseiten, die Links mit URLs, die mit "aim:" oder "ymsgr:" beginnen, enthalten. Das kann das Ausnutzen von Problemen in den URI-Handlern verhindern. Eine weitere Option ist die vorsichtige Entfernung von diesen Registry-Keys im Zweig "HKEY_CLASSES_ROOT".
 - Für AOL blockieren Sie das folgende Ziel: oscar.login.aol.com

- Für Google Talk blockieren Sie das folgende Ziel: talk.google.com
- Yahoo Instant Messenger tunnelt seinen Verkehr durch eine Vielzahl von Ports, inklusive finger, discard, chargen und SMTP. Um effektiv zu sein, blockieren Sie die folgenden Ziele zusätzlich zu den oben genannten Ports: cs.yahoo.com & scca.yahoo.com
- Verwenden Sie Richtlinien zur Softwareeinschränkungen oder andere Mechanismen um die Ausführung von IM Clients wie msmsgs.exe, aim.exe, ypager.exe, icq.exe, trillian.exe.
- Filtern Sie den HTTP Verkehr durch einen Proxyserver mit Anmeldung. Ein Proxyserver stellt Ihnen weitere Möglichkeiten um IM Verkehr zu filtern zur Verfügung.

C8.5 Weiterführende Informationen

Bedrohung durch Instant Messaging

IM Buffer Overflows

<http://www.sans.org/newsletters/risk/display.php?v=3&i=32#widely1> (AOL)

<http://www.sans.org/newsletters/risk/display.php?v=4&i=6#widely5> (Windows und MSN Messenger)
(MSN Messenger)

<http://www.sans.org/newsletters/risk/display.php?v=4&i=43#other1> (Skype)

C9. Mozilla und Firefox Browser

C9.1 Beschreibung

Mozilla Firefox Version 1.0 wurde offiziell im November 2004 veröffentlicht. Mozilla und Firefox sind als brauchbare Alternativen zum Internet Explorer aufgetaucht und haben stetig Marktanteile am Browsermarkt gewonnen. Mit der wachsenden Verbreitung wurden diese Browser genauer von Sicherheitsauditoren und Hackern untersucht, wodurch zahlreiche Schwachstellen im vergangenen Jahr entdeckt wurden. Viele der entdeckten Flaws sind sehr kritisch und ermöglichen es einer böartigen Webseite ein Clientsystem komplett zu kompromittieren. Exploit Code um diese Schwachstellen zu verwenden ist ebenso öffentlich verfügbar.

C9.2 Betroffene Betriebssysteme

Die Browser Mozilla und Firefox auf Windows und Linux Systemen

C9.3 CVE Einträge

[CVE-2005-0592](#), [CVE-2005-0593](#), [CVE-2005-0752](#), [CVE-2005-1155](#), [CVE-2005-1156](#), [CVE-2005-1157](#), [CVE-2005-1158](#), [CVE-2005-1160](#), [CVE-2005-1476](#), [CVE-2005-1477](#), [CVE-2005-1531](#), [CVE-2005-1937](#), [CVE-2005-2262](#), [CVE-2005-2267](#), [CVE-2005-2268](#), [CVE-2005-2269](#), [CVE-2005-2270](#), [CVE-2005-2602](#), [CVE-2005-2701](#), [CVE-2005-2705](#), [CVE-2005-2706](#), [CVE-2005-2707](#), [CVE-2005-2871](#), [CVE-2005-2968](#)

C9.4 Wie erkennt, ob man gefährdet ist, und sich vor diesen Schwachstellen schützen kann

- Wenn Sie Firefox oder Mozilla verwenden, aber nicht in der neuesten Version, dann sind Sie gefährdet. Firefox hat jetzt sowohl ein automatisches als auch ein manuelles Werkzeug mit dem man nach Updates suchen kann. Wie auch immer, Sie sollten regelmäßig die [Firefox](#) Site besuchen um die zeitgerechte Installation von Patches sicherzustellen.
- Verwenden Sie einen [Vulnerability Scanner](#) um gefährdete Installationen zu entdecken.
- Verwenden Sie [Intrusion Prevention/Detection Systeme](#) and [Antivirus- und Malware Detection Software](#) um böartigen HTML Scriptcode zu blockieren.

C9.5 Weiterführende Informationen

Mozilla Firefox Vulnerabilities

<http://www.sans.org/newsletters/risk/display.php?v=4&i=39#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=38#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=37#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=38#exploit1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=28#widely8>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=37#widely2>

C10. Andere Cross-platform Anwendungen

C10.1 Beschreibung

Dieser Abschnitt der Top-20 listet Schwachstellen in weitverbreiteten Produkten auf, die nicht in die anderen Kategorien passen. In den meisten Fällen können diese Schwachstellen von der Ferne ausgenutzt werden. Manche dieser Schwachstellen ermöglichen sogar unternehmensweite Beeinträchtigungen. Im Internet ist Exploit Code verfügbar, und es wurden Scans nach verwundbaren Systemen beobachtet.

- (a) Computer Associates License Manager Overflows ([CVE-2005-0581](#), [CVE-2005-0582](#), [CVE-2005-0583](#))
- (b) Novell eDirectory iMonitor und ZENWorks Buffer Overflows ([CVE-2005-2551](#), [CVE-2005-1543](#))
- (c) Computer Associates Message Queuing Vulnerabilities ([CVE-2005-2668](#))
- (d) Sun Java Security Vulnerabilities ([CVE-2004-1029](#), [CVE-2005-0418](#), [CVE-2005-0836](#), [CVE-2005-1973](#), [CVE-2005-1974](#))
- (e) HP Radia Management Software Overflows ([CVE-2005-1825](#), [CVE-2005-1826](#))
- (f) Snort BackOrifice Preprocessor Buffer Overflow ([CVE-2005-3252](#))
- (g) RSA SecurID Web Agent Overflow ([CVE-2005-1471](#))

C10.2 CVE Einträge

[CVE-2005-0581](#), [CVE-2005-0582](#), [CVE-2005-0583](#), [CVE-2005-2551](#), [CVE-2005-1543](#), [CVE-2005-2668](#), [CVE-2004-1029](#), [CVE-2005-0418](#), [CVE-2005-0836](#), [CVE-2005-1973](#), [CVE-2005-1974](#), [CVE-2005-1825](#), [CVE-2005-1826](#), [CVE-2005-3252](#), [CVE-2005-1471](#)

C10.3 Wie erkennt, ob man gefährdet ist, und sich vor diesen Schwachstellen schützen kann

Wenn Sie diese Produkte ohne die neuesten Patches verwenden, sind Sie verwundbar. Installieren Sie die Patches vom Hersteller um diese Schwachstellen zu beheben. Work-arounds sind im SANS @RISK Newsletter angeführt.

C10.4 Weiterführende Informationen

CA License Manager Overflows

<http://supportconnectw.ca.com/public/reglic/downloads/licensepatch.asp#alp>

http://supportconnectw.ca.com/public/ca_common_docs/security_notice.asp

<http://www.sans.org/newsletters/risk/display.php?v=4&i=9#widely1>

Novell eDirectory iMonitor und ZENWorks Overflow

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10098568.htm>

<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2972038.htm>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=33#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=20#widely1>

Computer Associates Message Queuing Vulnerabilities

<http://archives.neohapsis.com/archives/bugtraq/2005-08/0292.html>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=34#widely1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=42#exploit2>

Sun Java Security Vulnerabilities

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57740-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101748-1>

<http://sunsolve.sun.com/search/document.do?assetkey=1-26-101749-1>

<http://www.sans.org/newsletters/risk/display.php?v=3&i=47#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=12#widely2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=24#widely10>

HP Radia Management Software Overflows

<http://archives.neohapsis.com/archives/bugtraq/2005-06/0009.html>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=22#other1>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=18#other2>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=30#exploit1>

Snort BackOrifice Preprocessor Overflow

<http://www.snort.org/pub-bin/snortnews.cgi#99>

<http://www.sans.org/newsletters/risk/display.php?v=4&i=42#widely1>

Hauptschwachstellen in UNIX Systemen

U1. Schwachstellen in UNIX Konfigurationen

U1.1 Beschreibung

Die meisten Unix/Linux-Systeme enthalten in ihrer Standardinstallation zahlreiche Standarddienste. Über die Jahre haben sicherheitsbewusste Administratoren entweder nicht benötigte Dienste abgedreht oder trennen diese durch Firewalls für dem Internet. Der Abschnitt mit weiterführenden Informationen verweist auf detaillierte Zusammenfassungen über Unix-Konfigurationen im Allgemeinen.

Dieses Jahr sind Attacken gegen SSH besonders interessant. SSH ist ein interaktiver Dienst, der auf den meisten UNIX-Systemen verfügbar ist. Da dieser Dienst Daten, die über das Netzwerk transportiert werden, verschlüsselt, wird angenommen, daß dieser Dienst, wenn er auf dem aktuellen Patchlevel ist, sicher ist. Allerdings war das einer der Dienste, die im vergangenen Jahr sehr häufig mit Brute-Force Password-Guessing Angriffen angegriffen wurden. Systeme mit schwachen SSH-Passwörtern für normale Useraccounts werden bevorzugt beeinträchtigt; Eskalierung der Privilegien wird dann verwendet um Root-Zugriff zu erlangen und Root-Kits zu installieren um die Beeinträchtigung zu verstecken. Weiters ist es wichtig zu wissen, dass Brute-Force-Knacken von Passwörtern eine weitere Technik sein kann um sogar voll gepatchte Systeme zu beeinträchtigen. Es wird empfohlen, Public-Key-Authentisierungs-Mechanismen, die von den meisten SSH-Implementierungen angeboten werden, verwenden um diese Attacken zu erschweren. Diese Attacken können auf andere interaktive Dienste wie Telnet, ftp, usw. ausgedehnt werden.

U1.2 Betroffene Versionen

Alle UNIX-Versionen sind potentiell durch unsaubere oder Standardinstallationen gefährdet. Alle Versionen können auch durch Benutzerkonten mit schwachen oder wörterbuchbasierten Passwörtern beeinträchtigt werden.

U1.3 Wie erkennt, ob man gefährdet ist

- Verwenden Sie keine Standardpasswörter für Accounts.
- Verwenden Sie keine schwachen Passwörter oder Passwörter, die auf Wörtern aus dem Wörterbuch basieren. Überprüfen Sie Ihre Rechner um sicherzustellen, daß Ihre Passwortpolicy eingehalten wird. Installieren Sie regelmäßig die neuesten Patches vom Hersteller um Schwachstellen in exponierten Diensten zu entschärfen. Patch Management ist ein wesentlicher Bestandteil des Risikomanagementprozesses.
- Reduzieren Sie die Zahl der Anmeldeversuche für exponierte Dienste.
- Reduzieren Sie die Benutzerkonten, die sich über das Netzwerk anmelden können; Root sollte keines dieser Konten sein. Überlegen Sie sich, Firewallregeln zu implementieren um einzuschränken von wo aus Anmeldungen, z.B. über SSH, stattfinden können.
- Verbieten Sie Accounts, die von mehreren Benutzern geteilt werden, und verwenden Sie keine allgemeinen Benutzernamen wie tester, guest, sysadmin, admin, usw.
- Zeichnen Sie fehlgeschlagene Anmeldeversuche auf. Eine große Zahl von fehlgeschlagenen Anmeldungen an ein System kann eine weitergehende Überprüfung des Systems nach sich ziehen um herauszufinden, ob das System kompromittiert.
- Überlegen Sie die Verwendung von zertifikatsbasierter Anmeldung.
- Wenn Ihr UNIX-System die Verwendung von PAM Authentisierungsmodulen gestattet, verwenden Sie PAM-Module, die die Stärke von Passwörtern überprüfen.
- Stellen Sie Dienste, die nicht Zugriff auf das Internet benötigen hinter eine Firewall.
- Verwenden Sie die Benchmarks des Center for Internet Security von www.cisecurity.org für Ihr Betriebssystem und die Dienste, die Sie verwenden. Überlegen Sie sich auch, Bastille zum Härten von Linux und HP-UX basierten Rechnern von www.bastille-linux.org zu verwenden.
- Überlegen Sie sich, wenn möglich, Dienste von deren Standardport zu übersiedeln.

U1.4 Weiterführende Informationen

SSH Brute Force Attacken und Gegenmaßnahmen

<http://isc.sans.org/diary.php?date=2004-11-04>
<http://isc.sans.org/diary.php?date=2004-11-02>
<http://isc.sans.org/diary.php?date=2004-09-11>
<http://isc.sans.org/diary.php?date=2004-08-30>
<http://isc.sans.org/diary.php?date=2004-08-29>
<http://isc.sans.org/diary.php?date=2004-08-22>
<http://seclists.org/lists/firewall-wizards/2005/Jun/0154.html>
<http://www.counterpane.com/alert-cis20040910-1.html>
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1094140,00.html
<http://www.frsirt.com/exploits/08202004.brutessh2.c.php>

Allgemeine UNIX Security Ressourcen

<http://www.cisecurity.org>
<http://www.bastille-linux.org>

U2. Mac OS X

U2.1 Beschreibung

Das Mac OS X wurde im April 2001 als solides UNIX-basiertes Betriebssystem veröffentlicht. Obwohl Mac OS X von Haus aus Sicherheitsmerkmale wie eingebaute Personal Firewalls, deaktivierte nicht benötigte Dienste oder einfache Möglichkeiten, die Sicherheit zu erhöhen, implementiert hat, warten auf den Anwender noch immer viele Schwachstellen.

Mac OS X enthält auch den Safari Webbrowser. In diesem Browser wurden zahlreichen Schwachstellen gefunden, und in bestimmten Fällen wurde auch Exploit Code veröffentlicht.

Apple veröffentlicht oft Mac OS X Sicherheitsupdatesammlungen heraus, die normalerweise Korrekturen für eine große Zahl von Schwachstellen mit Risikobewertungen von kritisch bis gering enthalten. Das erschwert die Verfolgung von Schwachstellen in diesem Betriebssystem, und der beste Weg um die Sicherheit sicherzustellen, ist die Installation der neuesten Sammlpatches.

U2.2 Wie man erkennt, ob man gefährdet ist

Von allen Standard- oder ungepatchten Installationen kann angenommen werden, dass sie verwundbar sind.

Die folgende Prozedur wird überprüfen ob neue Pakete vorhanden sind. Wenn Sie keine wichtigen Patches für Pakete vorfinden, dürften Sie sicher sein:

1. Wählen Sie Systemeinstellungen aus dem Apple-Menü.
2. Wählen Sie Software-Aktualisierung.
3. Klicken Sie auf Aktualisieren.
4. Kontrollieren Sie die verfügbaren Pakete.

Um den Prozess der Schwachstellenanalyse zu unterstützen, können Sie beliebige [Vulnerability Scanner](#) einsetzen.

U2.3. CVE Einträge

[CVE-2005-0126](#), [CVE-2005-0418](#), [CVE-2005-0970](#), [CVE-2005-1331](#), [CVE-2005-1337](#), [CVE-2005-1342](#), [CVE-2005-1721](#), [CVE-2005-2501](#), [CVE-2005-2502](#), [CVE-2005-2507](#), [CVE-2005-2518](#)

Safari:

[CVE-2005-1474](#), [CVE-2005-2516](#), [CVE-2005-2517](#), [CVE-2005-2522](#)

U2.4. Wie man sich vor Schwachstellen in Mac OS X schützen kann

- Stellen Sie sicher, daß Sie auf dem aktuellen Stand sind und alle Sicherheitsupdates für Appleprodukte installiert haben indem Sie das Softwareaktualisierungssystem einschalten, damit es automatisch nach von Apple veröffentlichten Softwareupdates suchen kann. Obwohl verschiedene Zeitpläne möglich sind, empfehlen wir, daß Sie das System für zumindest wöchentliche Überprüfungen konfigurieren. Für weitere Informationen über die Suche nach Updates und das Software Update System, schauen Sie bitte auf die Apple Software Updates Webseite - <http://www.apple.com/macosx/upgrade/softwareupdates.html>
- Um unerlaubten Zugriff auf Ihren Rechner zu verhindern, aktivieren Sie die eingebaute Personal Firewall. Wenn Sie auf Ihrem System Dienste verwenden, denen Sie externe Zugriffe gestatten, erlauben Sie sie gezielt.
- Es gibt viele exzellente Anleitungen um Mac OS X zu härten. Der CIS Benchmark für Mac OS X zählt Sicherheitskonfigurationen auf, die beim Härten des Betriebssystems hilfreich sind. Die von den Level-1 Benchmark Dokumenten vorgeschlagenen Aktionen werden fast sicher keine Dienste oder Anwendungen beeinträchtigen und sollten auf

