



Le venti vulnerabilità più critiche per la sicurezza in Internet

Versione 4.0 - Ottobre 2003
Localizzata da Data Security
Copyright 2001-2003, The SANS Institute

Introduzione

Le venti vulnerabilità più critiche per la sicurezza in Internet

La grande maggioranza dei worm e degli altri attacchi che provengono da Internet sono resi possibili dalle vulnerabilità presenti in un numero molto limitato di servizi dei più diffusi sistemi operativi.

Ciò si deve al fatto che coloro che effettuano gli attacchi agiscono in modo opportunistico, ovvero scelgono la strada più semplice e comoda, sfruttando le vulnerabilità più conosciute e impiegando gli strumenti di aggressione più efficaci e diffusi. Contano sul fatto che le organizzazioni spesso non pongono rimedio ai problemi e quindi spesso si conducono attacchi indiscriminati, scegliendo gli obiettivi dai risultati di una serie di scansioni in Internet per rilevare i sistemi vulnerabili.

La facile e distruttiva diffusione di worm come Blaster, Slammer e Code Red, ad esempio, può essere direttamente addebitata allo sfruttamento di vulnerabilità per le quali non sono state tempestivamente applicate le opportune correzioni.

Tre anni fa, Il SANS Institute e il National Infrastructure Protection Center (NIPC) presso l'FBI pubblicarono un documento che elencava Le dieci vulnerabilità più critiche per la sicurezza in Internet. Da allora migliaia di organizzazioni hanno utilizzato quella lista, e le sue evoluzioni in Venti vulnerabilità diffuse negli anni seguenti, come guida per risolvere rapidamente i buchi di sicurezza più pericolosi. I servizi vulnerabili che hanno favorito i tre esempi riportati sopra - i worm Blaster, Slammer e Code Red, come d'altra parte anche NIMDA - sono riportati su quella liste.

Questa versione aggiornata delle "Venti Vulnerabilità più critiche" è in effetti costituita da due liste di dieci: i dieci servizi di Windows e i dieci di Unix le cui vulnerabilità sono più frequentemente sfruttate condurre un attacco.

Sebbene vi siano migliaia di episodi di violazione della sicurezza che ogni anno colpiscono questi sistemi operativi, la stragrande maggioranza degli attacchi portati a termine sono diretti verso uno o più dei venti servizi considerati più vulnerabili.

Le Venti vulnerabilità più critiche è una lista delle vulnerabilità che richiedono un intervento immediato, ed è il risultato di un processo che riunisce assieme dozzine tra i principali esperti di sicurezza provenienti da molti paesi, da ambienti governativi, accademici e industriali.

Essi provengono dalle agenzie federali statunitensi più sensibili a problemi della sicurezza, dagli enti governativi di Gran Bretagna e Singapore, dai principali produttori di software per la sicurezza e dalle più importanti società di consulenza, dai migliori progetti universitari per la sicurezza, dal SANS Institute e da molte altre organizzazioni. L'elenco dei partecipanti è disponibile alla fine del presente documento.

L'elenco SANS/FBI delle venti vulnerabilità più critiche è un documento in continuo aggiornamento. Contiene istruzioni dettagliate e riferimenti ad informazioni supplementari utili per correggere i problemi di sicurezza. Nel momento in cui si scoprono minacce più critiche di quelle elencate o metodi di intrusione più diffusi o più comodi, vengono aggiornati l'elenco delle vulnerabilità e le istruzioni per rimediare; in questo processo il vostro contributo è sempre gradito. Questo documento si basa sul consenso di un'intera comunità: la vostra esperienza nel combattere le intrusioni e nell'eliminare le vulnerabilità può aiutare quelli che verranno dopo di voi. Inviare i vostri suggerimenti a info@sans.org, specificando "Top Twenty Comments" nell'oggetto dell'e-mail.

[top ^](#)

Note per i lettori:

Codici CVE

Ogni vulnerabilità menzionata è accompagnata dai codici della catalogazione CVE (Common Vulnerabilities and Exposures). Spesso sono riportati anche i numeri CAN, ovvero i codici delle vulnerabilità che sono candidate ad essere incluse nella lista CVE, ma non sono state ancora completamente verificate. Per ulteriori informazioni relative al progetto CVE, oggetto di numerosi riconoscimenti ufficiali, consultate l'indirizzo <http://cve.mitre.org>.

I codici CVE e CAN corrispondono alle vulnerabilità più importanti che devono essere verificate per ciascuna voce. Ogni vulnerabilità CVE è collegata all'elemento corrispondente del servizio ICAT di indicizzazione delle vulnerabilità del National Institute of Standards (<http://icat.nist.gov>). Per ciascuna vulnerabilità ICAT fornisce una breve descrizione, un elenco delle caratteristiche (ad esempio ambito dell'attacco e danno potenziale), un elenco dei nomi e delle versioni dei software vulnerabili e i collegamenti ai bollettini sulle vulnerabilità e alle informazioni sulle patch.

Porte da bloccare a livello di firewall

Alla fine del documento troverete una sezione aggiuntiva che presenta l'elenco delle porte più comunemente esplorate attaccate. Bloccando il traffico che passa attraverso le porte a livello di firewall o di altri dispositivi di protezione del perimetro della rete, potete ottenere uno strato di difesa aggiuntivo che vi aiuterà a tutelarvi da eventuali sviste o errori di configurazione. Tenete comunque presente che, anche se utilizzate un firewall per bloccare il traffico di rete diretto a una porta, essa non è protetta da possibili azioni causate da soggetti che si trovano già all'interno del perimetro, né dall'azione di hacker penetrati utilizzando altri metodi.

Ancora più sicura è la pratica di implementare per default a livello di firewall o di router delle regole di blocco (deny) di tutto ciò che non è esplicitamente permesso, piuttosto che bloccare una per una delle porte specifiche.

[top ^](#)

Le principali vulnerabilità per i sistemi Windows

- [W1 Internet Information Services \(IIS\)](#)
- [W2 Microsoft SQL Server \(MSSQL\)](#)
- [W3 Autenticazione di Windows](#)
- [W4 Internet Explorer](#)
- [W5 Servizi Windows di accesso remoto](#)
- [W6 Microsoft Data Access Components \(MDAC\)](#)
- [W7 Windows Scripting Host](#)
- [W8 Microsoft Outlook e Outlook Express](#)
- [W9 Condivisione di file Peer to Peer \(P2P\) in Windows](#)
- [W10 Simple Network Management Protocol \(SNMP\)](#)

Le principali vulnerabilità per i sistemi Unix

- [U1 BIND Domain Name System](#)
- [U2 Remote Procedure Call \(RPC\)](#)
- [U3 Web Server Apache](#)
- [U4 Autenticazione in Unix - Account senza password o con password deboli](#)
- [U5 Servizi in chiaro](#)
- [U6 Sendmail](#)
- [U7 Simple Network Management Protocol \(SNMP\)](#)
- [U8 Secure Shell \(SSH\)](#)
- [U9 Configurazioni non corrette dei servizi NIS/NFS](#)

- **U10 Open Secure Sockets Layer (SSL)**

[top ^](#)

Le principali vulnerabilità per i sistemi Windows (W)

W1 Internet Information Services (IIS)

W1.1 Descrizione:

Le installazioni di default di Internet Information Services (IIS) si sono dimostrate nel tempo vulnerabili a un certo numero di attacchi gravi. Gli effetti di queste vulnerabilità possono includere:

- Interruzione del servizio;
- Esposizione o compromissione di file o dati sensibili;
- Esecuzione di comandi arbitrari;
- Totale compromissione del server.

IIS utilizza una funzione di programmazione nota come ISAPI per associare i file che hanno determinate estensioni con delle DLL (note come filtri ISAPI). I preprocessori come ColdFusion e PHP utilizzano le ISAPI, e lo stesso IIS include molti filtri ISAPI per gestire funzioni come le Active Server Page (ASP), i server-side include (SSI) e la condivisione di stampanti via Web. Molti filtri ISAPI installati per default con IIS non sono necessari nella maggior parte delle installazioni e molti di quei filtri sono sfruttati per attacchi. Gli esempi di programmi maligni che usano questo meccanismo di propagazione includono i ben noti worm Code Red e Code Red 2.

Come molti altri Web server, IIS include delle applicazioni di esempio che sono state ideate per esemplificare le funzionalità del web server. Queste applicazioni non sono state progettate per operare in modo sicuro in un ambiente di produzione. Alcune applicazioni di esempio di IIS consentono di vedere da remoto i file o di sovrascrivere i file, o persino l'accesso remoto ad altre informazioni critiche del server, compresa la password di amministrazione.

Una installazione di IIS che non venga costantemente aggiornata è soggetta inoltre alle vulnerabilità scoperte dopo la data di rilascio. Tra queste vi sono le vulnerabilità [WebDAV ntdll.dll](#) in IIS 5.0, che permette attacchi di denial of service e può fornire la possibilità a qualsiasi visitatore del sito web di creare ed eseguire script sul server, e la vulnerabilità Unicode, che consente a qualsiasi visitatore del sito di eseguire comandi arbitrari sul web server semplicemente richiedendo degli URL costruiti ad hoc.

I componenti aggiuntivi di terze parti, come ColdFusion e php, possono introdurre in una installazione IIS ulteriori vulnerabilità, sia per configurazioni non corrette sia derivanti da vulnerabilità intrinseche nel prodotto.

Inoltre: Maggiori informazioni riguardo alle più recenti vulnerabilità di WebDAV ([CAN-2003-0109](#) [CA-2003-09](#)) sono disponibili ai seguenti indirizzi:

<http://www.cert.org/advisories/CA-2003-09.html>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0109>
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q241520>

W1.2 Sistemi operativi interessati

- Windows NT 4 (qualsiasi versione) con IIS 4
- Windows 2000 Server con IIS 5
- Windows XP Professional con IIS 5.1

Alla stesura di questo documento non sono state riscontrate vulnerabilità in Windows 2003 con IIS 6; ma è ragionevolmente prevedibile che saranno rilevate e comunicate delle vulnerabilità quando un numero significativo di ambienti di produzione adotterà questa nuova piattaforma.

W1.3 Riferimenti CVE/CAN

[CVE-1999-0264](#), [CVE-1999-0278](#), [CVE-1999-0874](#), [CVE-1999-0237](#), [CVE-1999-0191](#),
[CVE-2000-0770](#),
[CVE-2000-0778](#), [CVE-2000-0884](#), [CVE-2000-0886](#), [CVE-2000-0226](#), [CVE-2001-0151](#),
[CVE-2001-0241](#),
[CVE-2001-0333](#), [CVE-2001-0500](#), [CVE-2001-0507](#)

[CAN-1999-0509](#), [CAN-1999-0736](#), [CAN-1999-1376](#), [CAN-2002-0071](#), [CAN-2002-0073](#),
[CAN-2002-0079](#),
[CAN-2002-0147](#), [CAN-2002-0149](#), [CAN-2002-0150](#), [CAN-2002-0364](#), [CAN-2002-0419](#),
[CAN-2002-0421](#),
[CAN-2002-0422](#), [CAN-2002-0869](#), [CAN-2002-1180](#), [CAN-2002-1181](#), [CAN-2002-1182](#),
[CAN-2002-1309](#),
[CAN-2002-1310](#), [CAN-2003-0109](#), [CAN-2003-0223](#), [CAN-2003-0224](#), [CAN-2003-0225](#),
[CAN-2003-0226](#),
[CAN-2003-0227](#), [CAN-2003-0349](#)

W1.4 Come determinare se siete vulnerabili

Le installazioni di default e quelle a cui non siano state applicate tutte le patch dovranno essere considerate vulnerabili.

Gli amministratori di sistema e di rete incaricati dell'installazione di dovranno acquisire una certa familiarità con la vasta raccolta di strumenti e documentazione per la sicurezza di Microsoft che riguardano la gestione adeguata di Internet Information Server.

Il principale archivio di documentazione riguardo alla sicurezza di IIS è l'[Internet Information Server \(IIS\) Security Center](#).

È consigliabile scaricare ed eseguire il [Microsoft Baseline Security Analyzer](#), che contiene le procedure di rilevazione specificatamente dedicate a IIS.

Gli amministratori dovrebbero anche confrontare i propri sistemi con tutto ciò che è descritto nelle diverse [checklist](#), [hardening guide](#) e nella documentazione per la [vulnerability remediation](#) che Microsoft mette a disposizione per valutare lo stato di vulnerabilità.

W1.5 Come proteggersi

Applicate le patch al sistema e mantenetele sempre aggiornate.

Applicare le patch al server al momento dell'installazione è un'operazione necessaria ma non sufficiente. Quando vengono scoperti nuovi difetti di IIS, dovrete applicare la patch conseguente. Per installazioni su un singolo server, potete scegliere di utilizzare Windows Update e AutoUpdate. [HFNetChk](#), il Network Security Hotfix Checker, assiste gli amministratori di sistema nell'analisi di sistemi locali o remoti per la verifica delle patch da aggiornare. Tale strumento funziona su Windows NT 4, Windows 2000 e Windows XP. La versione attuale può essere scaricata da Microsoft all'indirizzo <http://www.microsoft.com/technet/security/tools/hfnetchk.asp>.

Se utilizzate componenti aggiuntivi di terze parti come ColdFusion, PerlIIS o PHP, ricordate di controllare costantemente sui siti web dei rispettivi produttori la presenza di patch e di consigli per la configurazione. Per ovvie ragioni, Microsoft non include le patch di terze parti in servizi come Windows Update e strumenti simili.

Utilizzate IIS Lockdown Wizard per rafforzare l'installazione

Microsoft ha rilasciato un semplice strumento, noto come IIS Lockdown Wizard, che aiuta a rendere più sicure le installazioni di IIS. La versione più recente può essere scaricata da Microsoft all'indirizzo <http://www.microsoft.com/technet/security/tools/locktool.asp>.

L'esecuzione di IIS Lockdown Wizard in modalità "custom" o "expert" vi permetterà di operare le seguenti modifiche consigliate a qualsiasi installazione di IIS:

- Disabilitare WebDAV (a meno che il vostro ambiente non lo richieda inderogabilmente per la pubblicazione dei contenuti web).
- Disabilitare tutte le estensioni ISAPI non necessarie (in particolare .htr, .idq, .ism e .printer).
- Eliminare le applicazioni di esempio.
- Impedire al web server di eseguire comandi di sistema usati comunemente per acquisirne il controllo (es. cmd.exe e ftp.exe).

Utilizzate URLScan per filtrare le richieste HTTP

Molti exploit di IIS, incluse le famiglie di Code Blue e Code Red, utilizzano richieste HTTP articolate appositamente per operare attacchi Unicode o buffer overflow. È possibile configurare il filtro URLScan per respingere tali richieste prima che il server tenti di processarle. La versione più recente di URLScan è integrata nel IIS Lockdown Wizard, ma può essere anche scaricata separatamente da Microsoft all'indirizzo <http://www.microsoft.com/technet/security/tools/urlscan.asp>.

[indice ^](#)

W2 Microsoft SQL Server (MSSQL)

W2.1 Descrizione

Microsoft SQL Server (MSSQL) contiene numerose vulnerabilità gravi che permettono ad aggressori remoti di ottenere informazioni riservate, di alterare il contenuto del database, di compromettere i server SQL e, in alcune configurazioni, anche gli host.

Le vulnerabilità di MSSQL sono molto pubblicizzate e ancora sotto attacco. Due recenti worm MSSQL, diffusi rispettivamente nel Maggio 2002 e a Gennaio 2003, sfruttavano numerose vulnerabilità note di MSSQL. Gli host compromessi da questi worm generano un traffico di rete estremamente dannoso quando analizzano la rete alla ricerca di altri host vulnerabili. Ulteriori informazioni possono essere reperite agli indirizzi:

SQLSnake/Spida Worm (Maggio 2002)

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

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

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

Le porte 1433 e 1434 (le porte di default del server e del monitor MSSQL) sono regolarmente registrate presso l'[Internet Storm Center](#) come due delle porte più sondate in assoluto.

Il funzionamento dell'exploit di SQLSnake è legato alla presenza di un account di amministrazione, o "sa" account, che abbia una password nulla. È fondamentale per una

configurazione corretta e per la sicurezza di qualsiasi sistema accertarsi sempre che tutti gli account siano protetti da password oppure completamente disabilitati, se non sono usati. Potete trovare ulteriori informazioni riguardo alle impostazioni e alla gestione delle password degli account nella documentazione della Microsoft Developer Network sotto [Changing the SQL Server Administrator Login](#), oppure sotto [Verify and Change the System Administrator Password by Using MSDE](#). Gli account dovrebbero avere una password piuttosto complessa e difficile da individuare, anche se non sono utilizzati per eseguire la vostra implementazioni SQL/MSDE.

Il funzionamento dell'exploit di Slammer si basa su un buffer overflow nel Resolution Service di SQL Server. Questo buffer overflow ha effetto e di conseguenza la sicurezza dell'host è compromessa quando il worm invia dei particolari pacchetti di attacco verso la porta UDP 1434 dei sistemi vulnerabili. Se la macchina esegue servizi SQL che sono soggetti a buffer overflow e riceve questi pacchetti, il risultato è di solito una totale compromissione della sicurezza del server e del sistema. Le più efficaci misure di sicurezza contro questo worm sono costituite dall'applicare diligentemente tutte le patch, nell'utilizzare procedure di configurazione che prevengano il problema e il filtraggio in entrata e in uscita della porta UDP 1434 già a livello di accesso alla rete.

Il Microsoft Server 2000 Desktop Engine (MSDE 2000) può essere considerato un "SQL Server Lite". Molti non sono a conoscenza che i propri sistemi eseguono MSDE e che hanno installato una versione di SQL Server. MSDE 2000 viene installato assieme ai seguenti prodotti Microsoft:

1. SQL/MSDE Server 2000 (versione Developer, Standard e Enterprise)
2. Visual Studio .NET (versione Architect, Developer e Professional)
3. ASP.NET Web Matrix Tool
4. Office XP
5. Access 2002
6. Visual Fox Pro 7.0/8.0

Oltre a quelli elencati, anche molti altri pacchetti software possono far uso di MSDE 2000. Per una lista aggiornata, controllate all'indirizzo <http://www.SQLsecurity.com/forum/applicationslistgridall.aspx>. Dal momento che questi software utilizzano MSDE come core database engine, presentano necessariamente le stesse vulnerabilità di SQL/MSDE Server. MSDE 2000 può essere configurato per ricevere le connessioni client in entrata in molti modi diversi. Può essere configurato in modo che i client utilizzino le named pipe attraverso una sessione NetBIOS (porte TCP 139/445) o si connettano tramite un socket alla porta 1433 TCP, o entrambi. A prescindere dal metodo utilizzato, SQL Server e MSDE saranno comunque sempre in ascolto sulla porta 1434. Questa porta è definita come porta di controllo. I client invieranno un messaggio a questa porta per scoprire dinamicamente come connettersi al server.

Il motore MSDE 2000 restituisce informazioni che lo riguardano ogni qualvolta arriva un singolo pacchetto single byte 0x02 sulla porta UDP 1434. Altri pacchetti single byte causano un buffer overflow senza doversi mai autenticare presso il server. Ciò che complica questo problema è che l'attacco è condotto attraverso il canale UDP. Quando il processo di MSDE 2000 gira in un contesto sicuro di un utente del dominio o dell'account locale SYSTEM, lo sfruttamento riuscito di questi buchi di sicurezza può comportare una totale compromissione del sistema preso di mira.

Siccome SQL Slammer riesce a causare un buffer overflow sul sistema preso di mira, rispettare la buona abitudine di applicare periodicamente le patch e di configurare correttamente il sistema aiuta a mitigare questo pericolo. Scaricando e utilizzando strumenti di difesa come il [Microsoft SQL Critical Update Kit](#), si può verificare se i sistemi locali siano vulnerabili a questo exploit, analizzare interi domini o reti alla ricerca di sistemi vulnerabili e aggiornare automaticamente i file tramite l'SQL Critical Update.

Consulta i report e le analisi presenti su incidents.org per maggiori dettagli sul worm SQL/MSDE Slammer. Questo particolare attacco colpì per alcune ore la dorsale principale di Internet la mattina del 25 gennaio 2003.

W2.2 Sistemi operativi interessati

Qualsiasi sistema Microsoft Windows con installato Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 o Microsoft SQL/MSDE Server Desktop Engine 2000 e tutti quei sistemi che usano separatamente il motore MSDE.

W2.3 Riferimenti CVE/CAN

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

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

W2.4 Come determinare se siete vulnerabili

Microsoft ha pubblicato una serie di strumenti di sicurezza all'indirizzo <http://www.microsoft.com/sql/downloads/securitytools.asp>. Il kit denominato SQL Critical Update Kit contiene strumenti preziosi come SQL Scan, SQL Check e SQL Critical Update.

Chip Andrews di sqlsecurity.com ha rilasciato uno strumento chiamato SQLPingv2.2. Questo tool invia un pacchetto UDB single byte (valore byte di 0x02) verso la porta 1434 di un singolo host o di una intera sottorete. I Server SQL in ascolto sulla porta UDP 1434 rispondono rivelando dettagli del sistema come la versione del software, le istanze ecc. SQLPingv2.2 è considerato uno strumento di analisi e rilevazione molto simile a SQL Scan di Microsoft, e non influisce sulla sicurezza del sistema o della rete. Sul sito di Chip Andrews [SQL/MSDE Security](#) si trovano anche altri strumenti per la sicurezza di SQL.

W2.5 Come proteggersi

Sommario:

1. Disabilitate SQL/MSDE Server Monitor sulla porta 1434 UDP.
2. Applicate il più recente service pack per Microsoft SQL/MSDE server e/o MSDE 2000.
3. Applicate le patch cumulative più recenti rilasciate dopo l'ultimo service pack.
4. Applicate ciascuna singola patch rilasciata dopo la più recente patch cumulativa.
5. Abilitate l'Authentication Logging di SQL Server.
6. Rendete più sicuro il server a livello di sistema e a livello di rete.
7. Riducete al minimo i privilegi del servizio MSSQL/MSDE Server e di SQL/MSDE Server Agent.

In dettaglio:

1. Disabilitate SQL/MSDE Server Monitor sulla porta 1434 UDP.

Questa operazione può essere facilmente portata a termine installando e utilizzando le funzionalità comprese nel [SQL Server 2000 Service Pack 3a](#). Il database engine Microsoft MSDE 2000 presenta due vulnerabilità buffer overflow che possono essere sfruttate da un aggressore remoto senza nemmeno autenticarsi su server. Ciò che complica questo problema è che l'attacco è condotto attraverso il canale UDP.

Quando il processo di MSDE 2000 gira in un contesto sicuro di un utente del dominio o dell'account locale SYSTEM, lo sfruttamento riuscito di questi buchi di sicurezza può comportare una totale compromissione del sistema preso di mira. MS-SQL/MSDE Slammer invia un pacchetto UDP di 376 byte verso la porta 1434 utilizzando indirizzi di destinazione a caso e ripetendo l'operazione con alta frequenza. Il sistema compromesso, una volta infetto, inizia immediatamente a inviare a sua volta identici pacchetti da 376. Il worm invia il traffico a indirizzi IP casuali, includendo IP multicast, causando un Denial of Service della rete presa di mira. Singole macchine colpite dal worm hanno evidenziato dopo essere state infette un aumento del traffico dell'ordine di 50 Mb/sec.

2. Applicate il più recente service pack per Microsoft SQL/MSDE server e/o MSDE 2000.

Le versioni correnti dei service pack per il servizio Microsoft SQL/MSDE sono:

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

Per accertarvi di essere informati sui prossimi aggiornamenti, controllate regolarmente il documento di Microsoft Technet [Make Your SQL/MSDE Servers Less Vulnerable](#).

3. Applicate le patch cumulative più recenti rilasciate dopo l'ultimo service pack.

Le patch cumulative corrente per tutte le versioni di SQL/MSDE/MSDE Server è disponibile presso [MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks \(Q316333/Q327068\)](#).

Per accertarvi di essere informati sui prossimi aggiornamenti, controllate l'uscita di nuove patch cumulative per Microsoft SQL/MSDE Server agli indirizzi:

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

4. Applicate ciascuna singola patch rilasciata dopo la più recente patch cumulativa.

Attualmente non vi sono patch singole rilasciate dopo la MS02-061 Elevation of Privilege in SQL/MSDE Server Web Tasks (Q316333/Q327068). Per restare al passo con i prossimi aggiornamenti, verificate la presenza di nuove patch singole agli indirizzi:

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

5. Abilitate l'Authentication Logging di SQL Server.

L'Authentication Logging di SQL Server di solito non è abilitato. Questa operazione può essere effettuata tramite l'Enterprise Manager (Server properties; sezione Security).

6. Rendete più sicuro il server a livello di sistema e a livello di rete.

Una delle vulnerabilità MSSQL più frequentemente attaccate riguarda il fatto che l'account di amministrazione di default (noto come "sa") viene installato con password vuota. Se il vostro account "sa" di SQL/MSDE non è protetto da password, non potete ritenervi sicuri e potete cadere vittima di worm o di altri exploit. Perciò seguite le raccomandazioni raccolte alla voce "System Administrator (SA) Login" in [SQL/MSDE Server Books Online](#) per assicurarvi che l'account "sa" installato abbia una password sufficientemente robusta, e questo anche se il vostro server SQL/MSDE non usa tale account.

Sulla Microsoft Developer's Network è presente la documentazione su come cambiare il login di amministratore ([Changing the SQL Server Administrator Login](#)) e su come verificare e cambiare la password di amministratore usando MSDE ([Verify and Change the System Administrator Password by Using MSDE](#))

7. Riducete al minimo i privilegi del servizio MSSQL/MSDE Server e di SQL/MSDE Server Agent.

Eseguite il servizio MSSQL/MSDE Server e l'SQL/MSDE Server Agent sotto un account valido di dominio con privilegi minimi, non come amministratore del dominio

o con l'account SYSTEM (su NT) o LocalSystem (su 2000 or XP). Se il servizio compromesso viene eseguito con privilegi locali o di dominio permette all'aggressore di ottenere il controllo completo della vostra macchina e/o della vostra rete.

- a. Abilitate l'Autenticazione Windows NT, abilitate la verifica dei login effettuati e falliti e quindi fermate e riavviate il servizio MSSQL/MSDE Server. Se possibile, configurate i client in modo che usino l'Autenticazione NT.
- b. Si raccomanda un'azione di packet filtering effettuata a livello perimetrale in modo da bloccare le connessioni non autorizzate in entrata e in uscita agli specifici servizi MSSQL. Il filtering per l'ingresso dalle porte TCP/UDP 1433 e 1434 può prevenire l'azione di aggressori interni o esterni che attraverso queste porte possono effettuare scansioni o infettare eventuali server Microsoft SQL/MSDE vulnerabili residenti nella rete locale che non sono esplicitamente autorizzati a fornire servizi SQL/MSDE pubblici.
- c. Se i vostri servizi richiedono che le porte TCP 1433 e 1434 verso Internet debbano rimanere aperte, abilitate e personalizzate il filtering in ingresso e in uscita in modo da prevenire l'uso non corretto di queste porte.

Ulteriori informazioni su come rendere più sicuro Microsoft SQL/MSDE Server possono essere reperite agli indirizzi

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

[indice ^](#)

W3 Autenticazione di Windows

W3.1 Descrizione

In quasi tutte le interazioni tra gli utenti e i sistemi informativi vengono utilizzate password, frasi identificative o codici di sicurezza. La maggior parte delle forme di autenticazione, come la maggior parte delle protezioni per file e dati, si basa su password fornite dall'utente. Dal momento che gli accessi correttamente autenticati spesso non vengono registrati, o anche se vengono registrati non lo sono in modo da fornire alcun segnale di allarme, una password compromessa rappresenta un'opportunità potenziale di esplorare un sistema dall'interno senza essere identificati. Un aggressore avrebbe accesso completo a qualsiasi risorsa disponibile per quell'utente e sarebbe molto vicino ad essere in grado di accedere ad altri account, a macchine vicine e forse anche ad ottenere privilegi di amministrazione. Nonostante questi pericoli, gli account con password deboli o addirittura senza password rimangono estremamente diffusi e le società con una buona policy sull'utilizzo delle password ancora troppo rare.

Le più comuni vulnerabilità delle password sono dovute a:

- Account utente senza password o con password deboli.
- Al fatto che, a prescindere dalla robustezza delle password, spesso gli utenti non le proteggono adeguatamente.
- Al fatto che il sistema operativo o il software applicativo creano account di amministrazione con password deboli o privi di password.
- Al fatto che gli algoritmi di hashing delle password sono noti e spesso gli hash vengono memorizzati in modo da essere accessibili a chiunque. La difesa migliore e la più corretta contro queste vulnerabilità è una solida policy che includa le istruzioni per creare delle buone password e che riassume i comportame