



Le venti vulnerabilità più critiche per la Sicurezza in Internet



Indice

PREFAZIONE	3
LE VULNERABILITÀ PIÙ CRITICHE PER TUTTI I SISTEMI (G)	6
G1 – INSTALLAZIONI PREDEFINITE DEI SISTEMI OPERATIVI E DELLE APPLICAZIONI	6
G2 – ACCOUNT SENZA PASSWORD O CON PASSWORD “DEBOLI”	7
G3 – BACKUP INESISTENTI O INCOMPLETI.....	9
G4 – NUMERO ELEVATO DI PORTE APERTE.....	10
G5 – I PACCHETTI NON VENGONO FILTRATI PER DETERMINARNE IL CORRETTO INDIRIZZO IN INGRESSO E IN USCITA.....	11
G6 – LOG INESISTENTI O NON COMPLETI	13
G7 – PROGRAMMI CGI VULNERABILI.....	14
LE VULNERABILITÀ PRINCIPALI DEI SISTEMI WINDOWS (W)	16
W1 - VULNERABILITÀ UNICODE (ATTACCO TRASVERSALE ALLE CARTELLE DEI SERVER WEB).....	16
W2 - ISAPI EXTENSION BUFFER OVERFLOW	17
W3 – VULNERABILITÀ IIS RDS (MICROSOFT REMOTE DATA SERVICES).....	19
W4 - NETBIOS - CONDIVISIONI WINDOWS DI RETE NON PROTETTE	19
W5 - PERDITA DI INFORMAZIONI CAUSATE DA CONNESSIONI CHE UTILIZZANO SESSIONI NULLE	21
W6 – HASHING DEBOLE NEL SAM (LM HASH):.....	22
LE VULNERABILITÀ PRINCIPALI DEI SISTEMI UNIX (U).....	24
U1 – BUFFER OVERFLOW NEI SERVIZI RPC:	24
U2 - VULNERABILITÀ DI SENDMAIL	25
U3 – VULNERABILITÀ DI BIND.....	26
U4 - COMANDI R.....	27
U5 - LPD (REMOTE PRINT PROTOCOL DAEMON)	27
U6 – SADMIND E MOUNTD	29
U7 - STRINGHE SNMP PREDEFINITE	30
APPENDICE A – PORTE GENERALMENTE VULNERABILI.....	31
APPENDICE B – GLI ESPERTI CHE CI HANNO AIUTATO A CREARE LE DIECI E LE VENTI VULNERABILITÀ PIÙ CRITICHE PER LA SICUREZZA IN INTERNET.....	32
APPENDICE C: VERSIONE ITALIANA.....	34

Prefazione

La pubblicazione e la divulgazione in Italia de “Le venti vulnerabilità più critiche per la sicurezza in Internet” è stata possibile grazie alla condivisione da parte del SANS Institute e di Data Security di una filosofia comune sulla sicurezza informatica.

L’idea fondamentale che ha portato a questa collaborazione è la convinzione che, per ridurre il rischio di attacchi informatici, sia necessario un continuo impegno nella ricerca delle vulnerabilità e nello sviluppo di contromisure adeguate e, contemporaneamente, un’opera di sensibilizzazione verso gli utenti e le aziende affinché non si trovino impreparati di fronte a questo tipo di minacce.

Ricerca, aggiornamento continuo e formazione devono essere gli ingredienti sempre presenti nell’attività di un’azienda che si occupi di sicurezza informatica.

In questo modo siamo in grado di proporre soluzioni tecnologiche all’avanguardia e, allo stesso tempo, appropriate alla specificità del cliente e al livello di maturità tecnologica ed informatica degli utenti.

La diffusione in Italia delle ricerche sulle vulnerabilità più comuni nei sistemi informatici è il risultato del nostro costante impegno nel settore della ricerca e della formazione.

Crediamo che, solo attraverso un’alleanza forte tra tutti coloro che nel mondo si occupano di sicurezza informatica, sia possibile fronteggiare quanti, ogni giorno, si organizzano e si preparano ad usare le tecnologie informatiche per azioni criminali.

Stephen Northcutt
Director of Training and Certification
The SANS Institute

Romano Favero
Direttore Data Security

Le venti vulnerabilità più critiche per la sicurezza in Internet

Versione 2.504 - 01 maggio 2002 - Localizzata da Data Security
Copyright 2001-2002, The SANS Institute

Il SANS Institute e il National Infrastructure Protection Center (NIPC) pubblicarono poco più di un anno fa l'elenco delle dieci vulnerabilità più critiche per la sicurezza. Il documento è stato da allora utilizzato da migliaia di organizzazioni come guida per risolvere rapidamente i buchi di sicurezza più pericolosi. Il primo ottobre 2001 è stato pubblicato un nuovo elenco che aggiorna ed amplia quello esistente. Le vulnerabilità trattate, ora diventate venti, sono state divise in tre categorie: vulnerabilità generali, vulnerabilità di Windows e vulnerabilità di UNIX.

Il valore del documento del SANS/FBI sulle venti vulnerabilità più critiche (SANS/FBI Top Twenty List) è confermato dal fatto che la maggioranza degli attacchi ai sistemi informatici condotti via Internet andati a buon fine è ricollegabile allo sfruttamento delle vulnerabilità di sicurezza elencate. Ad esempio, la compromissione dei sistemi del Pentagono a seguito dell'episodio di hacking Solar Sunrise e la facile e rapida diffusione dei worm Code Red e NIMDA possono essere collegati allo sfruttamento di alcune vulnerabilità presenti nella lista per le quali non sono state applicati le opportune patch.

Questo limitato numero di vulnerabilità software sono alla base della maggior parte degli attacchi andati a buon fine, semplicemente perché coloro che effettuano gli attacchi agiscono in modo opportunistico, ovvero scelgono la strada più semplice e comoda. Essi sfruttano le vulnerabilità di sicurezza più conosciute e impiegano gli strumenti di aggressione più efficaci e diffusi. Contano sul fatto che le organizzazioni non pongono rimedio ai problemi e quindi, spesso, dopo aver effettuato scansioni in Internet per rilevare i sistemi vulnerabili, conducono attacchi indiscriminati.

In passato, gli amministratori di sistema hanno ammesso che non correggevano queste vulnerabilità semplicemente perché non si sapeva quali fossero quelle più pericolose, ed erano troppo occupati per poterle eliminare tutte. Alcuni strumenti per la rilevazione delle vulnerabilità possono ricercare 300, 500 o addirittura 800 tipi di vulnerabilità, diluendo l'impegno dell'amministratore di sistema nell'assicurarsi che i sistemi siano protetti dagli attacchi più comuni. Per aiutare gli amministratori a circoscrivere il problema è stato redatto l'elenco delle venti vulnerabilità principali, frutto dell'esperienza di decine tra i maggiori esperti delle agenzie federali più sensibili alla sicurezza, dei maggiori produttori di software, delle più importanti aziende di consulenza, dei migliori progetti universitari per la sicurezza, del CERT/CC e del SANS Institute. L'elenco dei partecipanti è disponibile alla fine del presente documento.

Commenti e osservazioni su questo lavoro sono sempre graditi.

The SANS Institute

Cinque note per i lettori:

Nota 1. Aggiornamenti

L'elenco SANS/FBI delle venti vulnerabilità più critiche (Top Twenty SANS/FBI) è un documento in continuo aggiornamento. Contiene istruzioni dettagliate e riferimenti a 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.

Nota 2. Numeri della lista CVE

Ogni vulnerabilità menzionata è accompagnata dai numeri della catalogazione CVE (Common Vulnerabilities and Exposures). Possono essere presenti anche i numeri CAN, ovvero i numeri candidati ad essere inclusi nella lista CVE, ma non ancora completamente verificati. Per ulteriori informazioni relative al progetto CVE, oggetto di numerosi riconoscimenti ufficiali, fate riferimento a <http://cve.mitre.org>. Nella sezione che descrive le vulnerabilità generali per tutti i sistemi, i numeri CVE elencati sono solo esempi di alcune delle vulnerabilità trattate nella lista. Gli elenchi CVE che riportiamo non intendono, infatti, essere esaustivi. In ogni caso, per quanto riguarda le vulnerabilità di Windows e di UNIX, i numeri CVE indicano le vulnerabilità prioritarie da controllare per ciascun tipo.

Nota 3. Porte da bloccare a livello di firewall

Alla fine del documento troverete una sezione aggiuntiva che presenta l'elenco delle porte utilizzate dai servizi che vengono comunemente esplorati e attaccati. Bloccando il traffico che passa attraverso le porte di firewall o di altri dispositivi di protezione del perimetro della rete, potete ottenere un livello di difesa aggiuntivo che aiuta a tutelarvi da eventuali 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.

Nota 4. Procedure automatiche per la rilevazione delle venti vulnerabilità più critiche

In questo documento sono descritti i metodi manuali utilizzati per rilevare in un sistema le vulnerabilità del nostro elenco. Un approccio più pratico per la ricerca delle vulnerabilità UNIX e Windows – specialmente se applicate la regola aurea di controllare ogni nuovo sistema prima di collegarlo ad Internet e ricontrollate frequentemente tutti i vostri sistemi – è quello di utilizzare uno scanner automatico per la rilevazione delle vulnerabilità. Bob Todd, creatore dello scanner gratuito per Internet SARA, ne ha realizzato una versione speciale progettata per rilevare e segnalare le venti vulnerabilità più critiche dell'elenco SANS/FBI. La classifica dei 20 scanner migliori (Top 20 Scanner) può essere scaricata dal sito Web del Center for Internet Security all'indirizzo www.cisecurity.org. Per rilevare queste vulnerabilità si possono utilizzare anche diversi scanner commerciali. L'elenco di quelli che possiedono una funzionalità specifica per il rilevamento delle venti vulnerabilità più critiche sarà sempre aggiornato dal Sans Institute e a disposizione all'indirizzo www.sans.org.

Nota 5. Collegamenti all'indice delle vulnerabilità ICAT

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.

Le vulnerabilità più critiche per tutti i sistemi (G)

G1 – Installazioni predefinite dei sistemi operativi e delle applicazioni

G1.1 Descrizione:

La maggior parte dei software, inclusi i sistemi operativi e le applicazioni, contengono script o programmi di installazione. Compito di questi ultimi è rendere l'installazione dei sistemi il più rapida possibile, abilitando le funzioni più importanti e riducendo così al minimo il lavoro per l'amministratore. Per raggiungere questo scopo, gli script generalmente installano più componenti di quelli necessari alla maggior parte degli utenti. I produttori di software preferiscono abilitare funzioni aggiuntive non necessarie piuttosto che lasciare che sia l'utente ad installarle in caso di bisogno. Questo tipo di approccio, sebbene rappresenti una comodità per l'utente, è l'origine di molte delle vulnerabilità più pericolose, per il semplice fatto che gli utenti non aggiornano né applicano le patch di sicurezza alle componenti software che non sono utilizzate. Inoltre molti utenti non hanno la percezione di cosa in realtà venga installato e quindi lasciano nel sistema pericolosi programmi dimostrativi semplicemente perché non ne conoscono l'esistenza.

I servizi non corretti con patch di sicurezza costituiscono la via attraverso la quale spesso gli intrusi ottengono il controllo dei computer.

Per quanto riguarda i sistemi operativi, le installazioni predefinite introducono quasi sempre servizi estranei con le corrispondenti porte aperte. Gli aggressori usano queste porte per introdursi nei sistemi. Nella maggior parte dei casi, meno porte rimangono aperte, meno strade un aggressore può utilizzare per danneggiare la vostra rete. Per quanto riguarda le applicazioni, le installazioni predefinite di solito contengono programmi o script dimostrativi non necessari. Una delle vulnerabilità più gravi per i server Web è rappresentata dagli script dimostrativi, che vengono utilizzati dagli aggressori per compromettere il sistema o per ottenere informazioni su di esso. Nella maggioranza dei casi, l'amministratore dei sistemi compromessi non sa o non ricorda di aver installato gli script dimostrativi. Gli script dimostrativi costituiscono un problema perché, di solito, non sono sottoposti alle stesse procedure di controllo di qualità adottate per gli altri software. In molti casi infatti la qualità del codice è incredibilmente scadente. Il controllo degli errori viene spesso tralasciato e così gli script sono terreno fertile per gli attacchi di tipo "buffer overflow".

G1.2 Sistemi interessati:

La maggior parte dei sistemi operativi e delle applicazioni. Tenete presente che quasi tutte le estensioni per server Web vengono fornite con file dimostrativi, molti dei quali sono estremamente pericolosi.

G1.3 Lista CVE:

(Nota: la lista sottostante non è da considerarsi completa o esaustiva. Contiene solo esempi di alcune delle vulnerabilità appartenenti alla categoria in questione).

[CVE-1999-0415](#), [CVE-1999-0678](#), [CVE-1999-0707](#), [CVE-1999-0722](#), [CVE-1999-0746](#),
[CVE-1999-0954](#), [CVE-2000-0112](#), [CVE-2000-0192](#), [CVE-2000-0193](#), [CVE-2000-0217](#),
[CVE-2000-0234](#), [CVE-2000-0283](#), [CVE-2000-0611](#), [CVE-2000-0639](#), [CVE-2000-0672](#),
[CVE-2000-0762](#), [CVE-2000-0868](#), [CVE-2000-0869](#), [CVE-2000-1059](#)

G1.4 Come determinare se siete vulnerabili:

Il vostro sistema è vulnerabile agli attacchi da parte degli hacker se avete usato un programma per l'installazione di software di sistema o di supporto (cosa che certamente si è verificata in quasi tutte le aziende) senza aver rimosso i servizi non necessari e senza aver installato tutte le patch di sicurezza.

Potreste essere vulnerabili anche se avete eseguito procedure di configurazione supplementari. Dovreste eseguire una scansione delle porte e una scansione delle vulnerabilità per ciascun sistema che debba essere collegato a Internet. Quando analizzate i risultati, tenete presente il principio per il quale il sistema dovrebbe eseguire il numero minimo di servizi e di pacchetti software indispensabile per svolgere le attività richieste. Ogni altro programma o servizio può diventare uno strumento per gli aggressori – in particolar modo perché la maggior parte degli amministratori di sistema non applica le patch necessarie ai servizi o ai programmi che non vengono di solito utilizzati.

G1.5 Come proteggersi:

Rimuovete il software non necessario, disattivate i servizi non necessari e chiudete le porte inutili. Senza dubbio può essere un compito lungo e tedioso. Proprio per questa ragione molte grosse organizzazioni hanno sviluppato linee guida di installazione standard per tutti i sistemi operativi e le applicazioni utilizzate all'interno dell'organizzazione. Queste prevedono l'installazione solo delle caratteristiche minime necessarie per un efficace funzionamento del sistema.

Il Center for Internet Security (CIS), basandosi sull'esperienza e le conoscenze di più di 170 organizzazioni appartenenti a una decina di paesi, ha stabilito una configurazione base di sicurezza per Solaris e Windows 2000 (vedi www.cisecurity.org). Strumenti per la valutazione delle prestazioni e per la verifica degli altri sistemi operativi sono in fase di sviluppo. Con gli strumenti del CIS si può verificare il livello di sicurezza di un sistema ed effettuare poi dei confronti tra i sistemi presenti nelle varie divisioni aziendali. Le linee guida del CIS possono essere seguite per migliorare la sicurezza della maggior parte dei sistemi operativi.

G2 – Account senza password o con password “deboli”

G2.1 Descrizione:

La maggior parte dei sistemi è configurata per utilizzare le password come prima ed unica linea di difesa. Gli user ID sono abbastanza facili da ottenere e la maggioranza delle aziende è dotata di un accesso dial-up che scavalca il firewall. Quindi, se un aggressore riesce a determinare il nome di un account e la sua password, potrà tranquillamente connettersi alla rete. Se un grosso problema è rappresentato dalle password facili da indovinare e da quelle predefinite, un problema ancora maggiore è dato dagli account del tutto privi di password. In pratica, tutti gli account che utilizzano password deboli, password predefinite oppure che non utilizzano alcuna password, dovranno essere rimossi dal sistema.

Inoltre, molti sistemi sono dotati di account incorporati o predefiniti. Di solito gli account di questo tipo usano le stesse password per tutte le installazioni di software. Gli aggressori vanno di solito alla ricerca di queste password, ben note nella comunità degli hacker. Per questo motivo anche gli account predefiniti o incorporati devono essere identificati e rimossi dal sistema.

G2.2 Sistemi interessati:

Tutti i sistemi operativi o le applicazioni dove gli utenti effettuano l'autenticazione con user ID e password.

G2.3 Lista CVE:

(Nota: la lista sottostante non è da considerarsi completa o esaustiva. Contiene solo esempi di alcune delle vulnerabilità appartenenti alla categoria in questione).

[CVE-1999-0291](#), [CAN-1999-0501](#), [CAN-1999-0502](#), [CAN-1999-0503](#), [CAN-1999-0505](#),
[CAN-1999-0506](#), [CAN-1999-0507](#), [CAN-1999-0508](#), [CAN-1999-0516](#), [CAN-1999-0517](#),
[CAN-1999-0518](#), [CAN-1999-0519](#)

G2.4 Come determinare se siete vulnerabili:

Per determinare se siete vulnerabili dovete conoscere gli account presenti nel vostro sistema. Quelle che seguono sono le operazioni che dovete compiere:

1. Verificate gli account presenti sui vostri sistemi e create un elenco principale. Non dimenticate di controllare le password su sistemi come router e stampanti digitali connesse a Internet, controller delle stampanti e delle copiatrici.
2. Sviluppate procedure per l'aggiunta di account autorizzati all'elenco e per la rimozione degli account non più in uso.
3. Controllate regolarmente l'elenco per accertarvi che non siano stati aggiunti nuovi account e che gli account inutilizzati siano stati rimossi.
4. Utilizzate uno strumento di password cracking per individuare gli account con password deboli o senza password. (Assicuratevi di avere un permesso ufficiale scritto prima di utilizzare lo strumento password cracking).
 - a. *LC3* – Microsoft Windows NT e Microsoft Windows 2000, <http://www.atstake.com>
 - b. *Microsoft Personal Security Advisor*, -- Microsoft Windows NT e Microsoft Windows 2000, www.microsoft.com/security/mpsa
 - c. *John the Ripper* – Unix, <http://www.openwall.com/john>
 - d. *Pandora* – Novell, <http://www.nmrc.org/pandora>
5. Impiegate procedure rigorose per la rimozione degli account di dipendenti o collaboratori che non lavorano più per l'organizzazione, o nel caso gli account non siano più necessari.

G2.5 Come proteggersi:

Per eliminare questi problemi di password è necessario applicare una procedura in due fasi. Nella prima fase è necessario che gli account senza password siano rimossi, o che sia loro assegnata una password, e che le password "deboli" siano irrobustite. Purtroppo accade spesso che gli utenti ai quali viene richiesto di modificare la propria password per renderla più robusta ne scelgano un'altra ugualmente facile da indovinare. Questo ci porta alla seconda fase della procedura, nella quale le password devono essere approvate dopo la modifica da parte dell'utente. Esistono programmi che controllano le password modificate e le rifiutano se non sono conformi ai requisiti stabiliti dalla vostra policy di sicurezza. I più diffusi sono descritti agli indirizzi elencati di seguito:

- 1a. Per UNIX: *Npasswd* (SunOS 4/5, Digital Unix, HP/UX e AIX)
<http://www.utexas.edu/cc/unix/software/npasswd>
- 1b. Per UNIX: "*Cracklib*" e i relativi moduli PAM (Linux)
2. Per Windows NT: *Passfilt*: <http://support.microsoft.com/support/kb/articles/Q161/9/90.asp>

Questi programmi garantiscono che le password modificate rispettino i criteri di composizione e di lunghezza necessari a renderle difficili da indovinare e da determinare. Molti produttori di sistemi Unix includono un supporto interno per l'irrobustimento delle password e sono comunque utilizzabili diversi pacchetti software dalle funzionalità simili.

Molte organizzazioni integrano i programmi per il controllo delle password con ulteriori controlli che ne garantiscono la modifica a intervalli regolari e l'impossibilità di riutilizzare le vecchie password. Se alle password viene applicata una scadenza, fate in modo che l'utente riceva un avviso e abbia la possibilità di modificare la password prima della scadenza. Quando si trovano davanti a un messaggio del tipo "la

vostra password è scaduta e deve essere modificata” gli utenti tendono a scegliere una password poco robusta.

Microsoft Windows 2000, nei Criteri di gruppo, offre opzioni per vincolare la scelta delle password. L'amministratore può configurare la rete affinché le password degli utenti rispettino una lunghezza minima, una durata minima e massima e altri tipi di vincoli. È importante impostare la durata minima di una password. Senza di essa, infatti, l'utente cambia la password dopo aver ricevuto l'avviso di scadenza che ne richiede la modifica, ma tende poi a modificarla nuovamente reimpostando quella preesistente. L'impostazione della durata minima fa in modo che gli utenti siano più propensi a ricordare la nuova password, e li scoraggia dal sostituirla con quella precedente.

Un'altra integrazione importante è costituita dai corsi di orientamento per aiutare gli utenti a capire perché sia necessaria scegliere password “robuste” e insegnare loro come farlo. Il consiglio più comune per ottenere password efficaci è quello di scegliere un verso di una canzone che contenga un numero e poi costruire la password utilizzando la prima o seconda lettera di ogni parola che non rappresenti un numero e la cifra per i numeri. Per rendere la password ancora più difficile da determinare includete un segno di interpunzione.

Un'altro modo per proteggersi dalla mancanza di password o dalle password deboli è quello di utilizzare forme diverse di autenticazione, come ad esempio l'autenticazione con password generate da token o l'autenticazione biometrica. Quindi, se le password deboli vi causano problemi, utilizzate metodi alternativi per l'autenticazione degli utenti.

G3 – Backup inesistenti o incompleti

G3.1 Descrizione:

Dopo il verificarsi di un incidente (ed è normale che prima o poi un incidente si verifichi in quasi tutte le organizzazioni), per ripristinare le condizioni preesistenti sono necessari backup aggiornati e metodi di ripristino dei dati di provata efficacia. Alcune organizzazioni effettuano backup quotidiani ma non verificano mai il loro effettivo funzionamento. Altre creano policy e procedure per i backup, senza però definire policy e procedure per il ripristino dei dati. Spesso tali errori vengono evidenziati solamente dopo che i dati sono già stati distrutti o danneggiati da hacker che si sono introdotti nei sistemi.

Un secondo problema è dato dalla scarsa protezione fisica dei supporti di backup. I backup contengono le stesse informazioni sensibili presenti sul server, quindi devono essere protetti in modo analogo.

G3.2 Sistemi interessati:

Tutti i sistemi di importanza critica.

G3.3 Lista CVE:

Non applicabile.

G3.4 Come determinare se siete vulnerabili:

Deve essere creato un inventario di tutti i sistemi di importanza “critica”. Per ognuno dei sistemi identificati è necessario effettuare un'analisi dei rischi che identifichi i pericoli a cui è sottoposto. Le policy e le procedure per il backup devono fare chiaro riferimento a questi sistemi. Dopo aver verificato i sistemi, è necessario verificare se:

1. Sono state stabilite procedure di backup per questi sistemi?
2. La periodicità dei backup è accettabile?
3. Il backup di ciascun sistema è effettuato secondo le procedure?
4. I supporti di backup sono stati controllati per garantire che i dati vengano salvati correttamente?

5. I supporti di backup sono adeguatamente protetti sia all'interno dei locali, sia mediante servizi di archiviazione esterni?
6. Le copie dei sistemi operativi e delle utility per il ripristino (inclusi i codici per le licenze) sono archiviate in sedi diverse?
7. Le procedure di ripristino sono state verificate e approvate?

G3.5 Come proteggersi:

I backup devono essere effettuati con cadenza almeno giornaliera. Requisito minimo per la maggior parte delle organizzazioni è di effettuare un backup completo ogni settimana e backup incrementali ogni giorno. Almeno una volta al mese il supporto di backup deve essere verificato effettuando un ripristino su un server di prova per controllare che la procedura utilizzata sia corretta. Questi sono i requisiti minimi. Alcune aziende effettuano backup completi ogni giorno oppure diversi backup incrementali durante tutto l'arco della giornata. Le soluzioni di backup di massimo livello sono costituite da reti totalmente ridondanti con capacità di recupero degli errori (fail-over), come richiedono i sistemi finanziari e di e-commerce che operano in tempo reale, quelli che controllano infrastrutture critiche e alcune strutture militari.

G4 – Numero elevato di porte aperte

G4.1 Descrizione:

Sia gli utenti legittimi che gli intrusi si connettono ai sistemi attraverso le porte aperte. Più sono le porte aperte più possibilità vengono offerte a chi voglia collegarsi al vostro sistema. È quindi importante lasciare aperto solo il minimo numero di porte indispensabile perché il sistema funzioni correttamente. Tutte le altre porte devono essere chiuse.

G4.2 Sistemi interessati:

La maggior parte dei sistemi operativi.

G4.3 Lista CVE:

(Nota: la lista sottostante non è da considerarsi completa o esaustiva. Contiene solo esempi di alcune delle vulnerabilità appartenenti alla categoria in questione).

[CVE-1999-0189](#), [CVE-1999-0288](#), [CVE-1999-0351](#), [CVE-1999-0416](#), [CVE-1999-0675](#),
[CVE-1999-0772](#), [CVE-1999-0903](#), [CVE-2000-0070](#), [CVE-2000-0179](#), [CVE-2000-0339](#),
[CVE-2000-0453](#), [CVE-2000-0532](#), [CVE-2000-0558](#), [CVE-2000-0783](#), [CVE-2000-0983](#)

G4.4 Come determinare se siete vulnerabili:

In locale può essere eseguito il comando *netstat* per determinare quali porte siano aperte, ma un metodo più sicuro è dato dall'analisi del sistema effettuata con uno scanner esterno per l'analisi delle porte. L'operazione vi fornirà l'elenco di tutte le porte in ascolto. Se i risultati di *netstat* differiscono da quelli dati dall'analisi delle porte, dovrete ricercarne il motivo. Quando i due elenchi coincidono, verificate il motivo per il quale ogni singola porta sia aperta e quale servizio sia in esecuzione su ciascuna porta. Le porte aperte che non possono essere verificate o la cui apertura non è giustificata devono essere chiuse. L'elenco definitivo deve essere salvato e utilizzato per effettuare procedure di controllo e verifiche periodiche per evitare la presenza di porte estranee aperte.

Tra i tanti scanner per l'analisi delle porte, il più diffuso è *nmap*. La versione per Unix di *nmap* è disponibile presso: <http://www.insecure.org/nmap/>. Questa versione può essere compilata anche su sistemi NT. La versione NT di *nmap* è disponibile presso: <http://www.eeye.com/html/Research/Tools/nmapnt.html>. Si possono impiegare senza problemi anche port scanner diversi da quelli elencati. Indipendentemente dallo scanner utilizzato, DOVETE effettuare la scansione sia delle porte TCP che delle porte UDP per l'intero campo di distribuzione: 1-65.535.

Prima di effettuare scansioni complete delle porte sui sistemi all'interno di un'organizzazione dovrete ottenere un permesso scritto. Alcuni sistemi operativi, e in particolare i dispositivi con stack TCP/IP incorporati, possono presentare comportamenti imprevedibili se sottoposti a scansione. Se non viene dato alcun preavviso, la scansione può anche attivare sistemi interni di rilevazione delle intrusioni o firewall e può essere interpretata come un attacco vero e proprio.

G4.5 Come proteggersi:

Dopo aver determinato quali porte sono aperte, identificate il sottoinsieme minimo di porte che dovranno rimanere aperte affinché il sistema funzioni in maniera efficace, quindi chiudete tutte le altre porte. Per chiudere una porta trovate il servizio corrispondente e disattivatelo o rimuovetelo.

Nei sistemi Unix molti servizi sono controllati da *inetd* e dal corrispondente file di configurazione *inetd.conf*. *Inetd.conf* elenca i servizi in ascolto su una determinata porta e può essere spesso utilizzato per chiudere le porte stesse. La rimozione di un servizio da *inetd.conf* e il successivo riavvio di *inetd* fa in modo che la porta non sia più aperta. Altri servizi sono avviati da script eseguiti durante la fase di avvio (come ad esempio */etc/rc*, */etc/rc.local*, o gli script contenuti nelle cartelle */etc/rc**). Dal momento che i dettagli per la disattivazione degli script variano a seconda della versione di Unix, consultate la documentazione del sistema per le specifiche modalità di disattivazione. Per controllare e verificare le porte aperte sui sistemi Unix si può utilizzare anche il programma *lsof*, scaricabile da: <ftp://vic.cc.purdue.edu/pub/tools/UNIX/lsof/lsof.tar.gz>.

In Windows NT e 2000, per determinare i servizi/programmi in ascolto su una determinata porta, può essere utilizzato il programma *fport* (www.foundstone.com). In Windows XP, potete determinare quale programma sia in ascolto su una porta eseguendo il comando *netstat* con l'opzione *-o*. Le informazioni così ottenute vi consentiranno di disabilitare il servizio e, di conseguenza, di chiudere la porta.

G5 – I pacchetti non vengono filtrati per determinarne il corretto indirizzo in ingresso e in uscita

G5.1 Descrizione:

Lo spoofing degli indirizzi IP è un metodo comune utilizzato dagli aggressori per nascondere le tracce del proprio attacco. Il celebre attacco "smurf", ad esempio, sfrutta una proprietà dei router per inviare un flusso di pacchetti a migliaia di macchine. Ogni pacchetto ha l'indirizzo sorgente contraffatto e sostituito da quello di una vittima. I computer ai quali sono indirizzati i pacchetti saturano il computer della vittima (flooding), spesso bloccando il computer o la rete. Un alto livello di protezione può essere ottenuto filtrando il traffico in ingresso (ingress filtering) e in uscita (egress filtering) dalla vostra rete. Le regole per il filtering sono le seguenti:

1. I pacchetti in entrata alla vostra rete non devono avere un indirizzo sorgente appartenente alla vostra rete interna.
2. I pacchetti in entrata alla vostra rete devono avere un indirizzo di destinazione appartenente alla vostra rete interna.
3. I pacchetti in uscita dalla vostra rete devono avere un indirizzo sorgente appartenente alla vostra rete interna.
4. I pacchetti in uscita dalla vostra rete non devono avere un indirizzo di destinazione appartenente alla vostra rete interna.
5. I pacchetti in entrata o in uscita dalla vostra rete non devono avere un indirizzo sorgente o di destinazione appartenente ad un indirizzo privato appartenente allo spazio riservato RFC1918. Sono inclusi gli indirizzi *10.x.x.x/8*, *172.16.x.x/12* o *192.168.x.x/16* e la rete di loopback *127.0.0.0/8*.

6. Bloccate i pacchetti instradati alla sorgente (source routed packet) o i pacchetti con il campo delle opzioni IP impostato.
7. Devono essere bloccati anche gli indirizzi riservati, quelli con auto configurazione DHCP e Multicast:
 - 0.0.0.0/8
 - 169.254.0.0/16
 - 192.0.2.0/24
 - 224.0.0.0/4
 - 240.0.0.0/4

G5.2 Sistemi interessati:

La maggior parte dei sistemi operativi e dispositivi di rete.

G5.3 Lista CVE:

(Nota: la lista sottostante non è da considerarsi completa o esaustiva. Contiene solo esempi di alcune delle vulnerabilità appartenenti alla categoria in questione).

[CAN-1999-0528](#), [CAN-1999-0529](#), [CAN-1999-0240](#), [CAN-1999-0588](#)

G5.4 Come determinare se siete vulnerabili:

Provate ad inviare un pacchetto contraffatto (“spoofed”) e controllate se viene bloccato dal vostro firewall esterno o dal router. Il vostro dispositivo non solo dovrà bloccare il traffico, ma dovrà anche annotare nel file di log che i pacchetti contraffatti sono stati rifiutati. Notate comunque che quanto descritto apre la porta ad un nuovo attacco – la saturazione (flooding) del file di log. Assicuratevi che il sistema di generazione dei log possa gestire grossi carichi, per evitare che sia vulnerabile ad attacchi DOS. Per verificare la funzionalità di questo tipo di filtro possono essere utilizzati programmi come *nmap* per l’invio di pacchetti esca o pacchetti contraffatti (spoofed). Dopo aver impostato il filtro non datene per scontato il corretto funzionamento. Verificatene spesso la funzionalità.

G5.5 Come proteggersi:

Per difendersi da questo tipo di attacco è necessario impostare delle regole per il filtering sul vostro router o firewall esterno. Di seguito riportiamo le regole d’esempio per un router Cisco:

1. filtro in entrata o ingress filtering

```
interface Serial 0

    ip address 10.80.71.1 255.255.255.0
    ip access-group 11 in

access-list 11 deny 192.168.0.0 0.0.255.255

access-list 11 deny 172.16.0.0 0.15.255.255

access-list 11 deny 10.0.0.0 0.255.255.255

access-list 11 deny <your internal network>

access-list 11 permit any
```

2. filtro in uscita o egress filtering

```
interface Ethernet 0

    ip address 10.80.71.1 255.255.255.0
    ip access-group 11 in

access-list 11 permit <your internal network>
```

G6 – Log inesistenti o non completi

G6.1 Descrizione:

Una delle massime della sicurezza è “L’ideale è prevenire, ma investigare è un dovere”. Il semplice fatto che consentiate al traffico di fluire tra la vostra rete e Internet vi rende automaticamente vulnerabili ai tentativi di penetrazione nella vostra rete da parte degli hacker. Ogni settimana vengono scoperte nuove vulnerabilità e ci sono ben pochi metodi per difendersi da un attacco che sfrutta una vulnerabilità non ancora nota. Dopo aver subito un’aggressione, se non disponete dei log, avete poche probabilità di scoprire cosa abbiano fatto gli intrusi. Senza quelle informazioni la vostra organizzazione può solo scegliere se ricaricare completamente il sistema operativo dal supporto originale, e sperare che i backup dei dati siano integri, oppure correre il rischio di continuare ad utilizzare un sistema che potrebbe essere ancora sotto il controllo di un hacker.

Se non siete a conoscenza di cosa stia succedendo nella vostra rete, non potrete riconoscere un attacco. I file di log forniscono i dettagli di quello che sta accadendo, dei sistemi sotto attacco e di quelli danneggiati.

La registrazione delle attività nel file di log deve essere effettuata con regolarità per tutti i sistemi di importanza cruciale; dovete inoltre effettuare un backup del file registro, dato che non sapete quando potreste averne bisogno. La maggior parte degli esperti raccomanda di inviare tutti i log ad un server centrale che scriva i dati su un supporto di memorizzazione non riscrivibile, impedendo così che un intruso sovrascriva i file registro per evitare di essere scoperto.

G6.2 Sistemi interessati:

Tutti i sistemi operativi e dispositivi di rete.

G6.3 Lista CVE:

[CAN-1999-0575](#), [CAN-1999-0576](#), [CAN-1999-0578](#)

G6.4 Come determinare se siete vulnerabili:

Esaminate i log di sistema di tutti i sistemi principali. Se i registri sono inesistenti o se le operazioni di memorizzazione e backup non sono eseguite a livello centralizzato, allora siete vulnerabili.

G6.5 Come proteggersi:

Impostate tutti i sistemi affinché registrino le attività su file registro locali che poi invieranno ad un sistema remoto. Questa procedura assicura ridondanza e aggiunge un livello di sicurezza. Poi confrontate i due file registro. Eventuali differenze tra i file potrebbero indicare attività sospetta nel sistema. Questa operazione permette anche di eseguire un controllo incrociato sui file di log. Una particolare riga in un file registro di una singola macchina potrebbe non destare alcun sospetto, ma la stessa riga ripetuta per 50 server di un’organizzazione ad intervalli di un minuto può essere il segnale di un gravissimo problema.

Quando possibile, inviate le informazioni dei registri ad un dispositivo che utilizzi un supporto non riscrivibile.

G7 – Programmi CGI vulnerabili

G7.1 Descrizione:

La maggior parte dei server Web, inclusi Microsoft IIS e Apache, supportano le funzionalità dei programmi CGI (common gateway interface) per fornire interattività alle pagine Web e funzioni come la raccolta e la verifica di dati. Di fatto, la maggior parte dei server Web contiene (ed installa) programmi CGI dimostrativi. Sfortunatamente sono troppi i programmatori di CGI che non considerano il fatto che i loro programmi forniscono a qualsiasi utente di Internet un collegamento diretto al sistema operativo del computer sul quale è installato il server Web. I programmi CGI vulnerabili rappresentano un'attrattiva particolare per gli aggressori perché sono relativamente facili da individuare ed eseguire con i privilegi del software dello stesso server Web. È risaputo che i programmi CGI vulnerabili sono stati sfruttati per deturpare pagine Web, rubare numeri di carta di credito e creare backdoor per assicurare intrusioni successive. Dopo la violazione del sito Web del Dipartimento di Giustizia degli Stati Uniti, è stata condotta un'analisi approfondita che ha determinato che molto probabilmente ciò che aveva permesso la violazione era la vulnerabilità di un programma CGI. Le applicazioni dei server Web sono ugualmente vulnerabili a causa delle falle di sicurezza generate da programmatori inesperti o disattenti. Come regola generale, i programmi dimostrativi devono essere sempre rimossi dai sistemi di produzione.

G7.2 Sistemi interessati:

Tutti i server Web.

G7.3 Lista CVE:

(Nota: la lista sottostante non è da considerarsi completa o esaustiva. Contiene solo esempi di alcune delle vulnerabilità appartenenti alla categoria in questione).

[CVE-1999-0067](#), [CVE-1999-0346](#), [CVE-2000-0207](#), [CVE-1999-0467](#), [CAN-1999-0509](#),
[CVE-1999-0021](#), [CVE-1999-0039](#), [CVE-1999-0058](#), [CVE-2000-0012](#), [CVE-2000-0039](#),
[CVE-2000-0208](#), [CAN-1999-0455](#), [CAN-1999-0477](#)

G7.4 Come determinare se siete vulnerabili:

Siete vulnerabili se il vostro server Web ospita qualche codice dimostrativo. Se avete programmi CGI legittimi, controllate che la versione utilizzata sia l'ultima e quindi effettuate l'analisi del vostro sito con uno scanner per la rilevazione delle vulnerabilità. Simulando il comportamento di un aggressore, sarete preparati a proteggere i vostri sistemi. Per scoprire script CGI vulnerabili potete usare uno scanner per la rilevazione delle vulnerabilità CGI chiamato *whisker*, reperibile presso:

<http://www.wiretrip.net/rfp/>

G7.5 Come proteggersi:

Questi sono i rimedi principali da adottare come difesa da programmi CGI vulnerabili:

1. Rimuovete tutti i programmi CGI dimostrativi dal server Web di produzione.
2. Controllate e verificate i restanti script CGI e rimuovete quelli non sicuri da tutti i server Web.
3. Accertatevi che tutti i programmatori di CGI rispettino una severa policy per il controllo della lunghezza del buffer di input nei programmi CGI.
4. Applicate le patch per le vulnerabilità note che non possono essere rimosse.
5. Accertatevi che la cartella CGI bin non contenga compilatori o interpreti.
6. Rimuovete lo script "view-source" dalla cartella cgi-bin.

7. I server Web non devono essere in esecuzione con i privilegi di amministratore o di root. La maggior parte dei server Web può essere configurata per funzionare con account dotati di privilegi inferiori, come ad esempio "nobody".
8. Non configurate il supporto CGI sui server Web che non ne hanno bisogno.

Le vulnerabilità principali dei sistemi Windows (W)

W1 - Vulnerabilità Unicode (attacco trasversale alle cartelle dei server Web)

W1.1 Descrizione:

Unicode assegna un numero univoco a ciascun carattere, indipendentemente dalla piattaforma, dal programma e dalla lingua. Lo Standard Unicode è stato adottato dalla maggior parte dei produttori, compreso Microsoft. Inviando a un server IIS una URL, appositamente preparata, contenente una sequenza Unicode UTF-8 non valida, un aggressore può forzare il server ad uscire letteralmente da una directory e ad eseguire script arbitrari. Questo tipo di attacco è anche conosciuto come directory traversal attack (attacco trasversale alle cartelle).

Gli equivalenti Unicode di / e di \ sono, rispettivamente, %2f e %5c. Tuttavia, potete rappresentare questi caratteri anche utilizzando le sequenze cosiddette decodificate. Le sequenze decodificate sono rappresentazioni Unicode tecnicamente non valide, essendo più lunghe di quelle necessarie per rappresentare il carattere. Sia / che \ possono essere rappresentati con un singolo byte. Una rappresentazione decodificata, come ad esempio %c0%af al posto di / rappresenta il carattere utilizzando due byte. IIS non è stato concepito per eseguire controlli di sicurezza sulle sequenze decodificate. Perciò i controlli di sicurezza di Microsoft possono essere aggirati trasmettendo una URL con sequenza Unicode decodificata. Se la richiesta proviene da una cartella contrassegnata dai diritti di esecuzione, l'aggressore può fare in modo che i file eseguibili presenti sul server vengano avviati. Ulteriori informazioni sui rischi legati alla vulnerabilità Unicode possono essere reperite presso:

<http://www.wiretrip.net/rfp/p/doc.asp?id=57&face=2>

W1.2 Sistemi interessati:

Microsoft Windows NT 4.0 con IIS 4.0 e Windows 2000 server con IIS 5.0 che non abbiano installato il Service Pack 2.

W1.3 Lista CVE:

[CVE-2000-0884](#)

W1.4 Come determinare se siete vulnerabili:

Siete probabilmente vulnerabili se state usando una versione IIS non aggiornata. Il modo migliore per stabilire se siete vulnerabili è quello di eseguire *hfnetchk*. *Hfnetchk* è uno strumento creato per gli amministratori per la verifica del livello di aggiornamento di uno o più sistemi e funziona in rete. La vulnerabilità Unicode di attacco trasversale alle cartelle è stata corretta con i seguenti aggiornamenti:

- Q269862 - MS00-057;
- Q269862 - MS00-078;
- Q277873 - MS00-086;
- Q293826 - MS01-026;
- Q301625 - MS01-044;
- Windows 2000 Service Pack 2.

Se non è stato installato nessuno di questi aggiornamenti, il sistema risulta essere vulnerabile a quanto descritto.

Per una verifica più specifica, provate a lanciare questo tipo di attacco contro il vostro sistema e controllatene l'esito. Provate ad utilizzare il seguente comando contro il vostro server Web IIS:

<http://victim/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\>

Per la verifica ad un sistema specifico è possibile che dobbiate modificare la URL. Se avete rimosso la cartella scripts (operazione consigliata), questo comando non sarà eseguito. Al posto della cartella scripts indicata nel comando, potete verificare le funzionalità di un sistema creando una cartella temporanea con diritti di esecuzione, oppure utilizzando un'altra cartella con i diritti di esecuzione già impostati. È ad esempio possibile che la cartella scripts sia stata rimossa ma che sia presente una cartella chiamata cgi-bin. Effettuate la verifica sul vostro sistema usando quindi la cartella cgi-bin al posto della cartella scripts.

Se siete vulnerabili, questa URL vi restituirà l'elenco dei contenuti del drive C della macchina vulnerabile. In sostanza l'attacco che state effettuando contro il vostro sistema è simile all'attacco di un vero aggressore. L'unica differenza è data dal fatto che mentre voi impiegate un comando non-intrusivo (*dir*), un aggressore potrebbe causare seri danni oppure creare una backdoor nel sistema.

W1.5 Come proteggersi:

Per proteggersi da questo tipo di attacco è necessario installare gli ultimi aggiornamenti Microsoft. Per informazioni su come reperire gli aggiornamenti fate riferimento al Microsoft Security Bulletin:

<http://www.microsoft.com/technet/security/bulletin/MS00-078.asp>

Anche strumenti come *IIS Lockdown Tool* e *URLScan* possono difendervi da questa vulnerabilità. *IIS Lockdown Tool* è stato progettato per aiutare gli amministratori a isolare un server IIS ed è reperibile presso:

<http://www.microsoft.com/technet/security/tools/locktool.asp>

URLScan è un analizzatore che filtra le richieste HTTP. Per esempio, può essere utilizzato per filtrare richieste contenenti caratteri con codice UTF8. *URLScan* è reperibile presso:

<http://www.microsoft.com/technet/security/URLScan.asp>

W2 - ISAPI Extension Buffer Overflow

W2.1 Descrizione:

L'Internet Information Server (IIS) di Microsoft è il software per server Web utilizzato per la maggior parte dei siti Web ospitati su server Microsoft Windows NT e Windows 2000. All'installazione di IIS, vengono anche installate automaticamente diverse estensioni ISAPI. Le ISAPI, acronimo di Internet Server Application Programming Interface, consentono agli sviluppatori di aumentare le capacità dei server IIS mediante l'uso di DLL. Molte DLL, come ad esempio *idq.dll*, contengono errori di programmazione che le portano a effettuare controlli inesatti nella rilevazione degli errori. In particolare queste non bloccano le stringhe di input di lunghezza non accettabile. In quello che è conosciuto come attacco da buffer overflow, gli aggressori possono inviare dati alle DLL ed assumere il pieno controllo del server Web IIS.

W2.2 Sistemi interessati:

Il buffer overflow di *idq.dll* interessa il Microsoft Index Server 2.0 e l'Indexing Service in Windows 2000.

Il buffer overflow di *.printer* interessa Windows 2000 Server, Advanced Server e Server Data Center Edition con IIS 5.0 installato. Questa DLL vulnerabile è contenuta anche in Windows 2000 Professional, ma non è collegata come impostazione predefinita. Se possibile, dovrete per precauzione utilizzare i Criteri di Gruppo per disabilitare la stampa via Web sulle stazioni di lavoro (in Configurazione Computer:Modelli Amministrativi:Stampanti).

W2.3 Lista CVE:

[CVE-1999-0412](#), [CVE-2001-0241](#), [CAN-2000-1147](#), [CAN-2001-0500](#)

W2.4 Come stabilire se siete vulnerabili:

Siete probabilmente vulnerabili se sul vostro server Web non è installato almeno il Service Pack 2. Se non siete sicuri di quali aggiornamenti siano installati, prelevate ed eseguite *hfnetchk* da:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/hfnetchk.asp>

I seguenti aggiornamenti correggono il problema del *.printer* buffer overflow:

- Q296576 - MS01-026;
- Q300972 - MS01-033;
- Q301625 - MS01-044;
- Windows 2000 SP2;
- Q299444 – The Windows NT 4.0 Security Roll-up Package.

I seguenti aggiornamenti correggono il *idq.dll* buffer overflow:

- Q300972 - MS01-033;
- Q301625 - MS01-044;
- The Windows NT 4.0 Security Roll-up Package.

W2.5 Come proteggersi:

Installate gli ultimi aggiornamenti di Microsoft. Potete trovarli agli indirizzi:

- Windows NT 4.0:
<http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp>
- Windows 2000 Professional, Server e Advanced Server:
<http://www.microsoft.com/technet/security/bulletin/MS01-044.asp>
- Windows 2000 Datacenter Server:
Gli aggiornamenti per Windows 2000 Datacenter Server riguardano l'hardware e sono disponibili presso il produttore del dispositivo;
- Windows XP:
La vulnerabilità non riguarda Windows XP.

Inoltre, l'amministratore dovrebbe rimuovere le estensioni ISAPI non necessarie. Controllate regolarmente che le estensioni non siano state riassegnate.

Ricordando il principio delle autorizzazioni minime indispensabili, il vostro sistema deve utilizzare il numero minimo di servizi indispensabili al corretto funzionamento.

Sia *IIS Lockdown Tool* che *URLScan* sono in grado di proteggervi da questa vulnerabilità. *IIS Lockdown Tool*, uno strumento rivolto agli amministratori ed impiegato per isolare un server IIS, è disponibile presso:

<http://www.microsoft.com/technet/security/tools/locktool.asp>

URLScan è un analizzatore che può filtrare molti tipi di richieste HTTP. Per esempio, può essere usato per filtrare richieste contenenti codici di caratteri UTF8. *URLScan* è reperibile presso:

<http://www.microsoft.com/technet/security/URLScan.asp>

W3 – Vulnerabilità IIS RDS (Microsoft Remote Data Services)

W3.1 Descrizione:

L'Internet Information Server (IIS) di Microsoft è il software per server Web utilizzato per la maggior parte dei siti Web ospitati su server Microsoft Windows NT 4.0. Gli utenti malintenzionati sfruttano i difetti di programmazione presenti nei Remote Data Services (RDS) di IIS per eseguire comandi remoti con i privilegi di amministratore.

W3.2 Sistemi interessati:

I sistemi Microsoft Windows NT 4.0 con Internet Information Server hanno la directory virtuale */msadc* collegata e vi sono molte probabilità che siano vulnerabili.

W3.3 Annotazioni Lista CVE:

[CVE-1999-1011](http://www.cve.org/CVE/1999/1011)

W3.4 Come stabilire se siete vulnerabili:

Se adoperate un sistema non aggiornato, siete vulnerabili.

Una guida eccellente ai punti deboli di RDS e ai metodi per correggerli può essere trovata in: <http://www.wiretrip.net/rfp/p/doc.asp?id=29&iface=2>.

W3.5 Come proteggersi:

Non è possibile eliminare la vulnerabilità con un aggiornamento. Per proteggersi è necessario seguire le indicazioni dei seguenti bollettini di sicurezza:

- <http://support.microsoft.com/support/kb/articles/q184/3/75.asp>
- <http://www.microsoft.com/technet/security/bulletin/ms98-004.asp>
- <http://www.microsoft.com/technet/security/bulletin/ms99-025.asp>

In alternativa, potete evitare il problema aggiornando i Microsoft Data Access Components (MDAC) ad una versione superiore alla 2.1. Le versioni più recenti di MDAC sono disponibili all'indirizzo: <http://www.microsoft.com/data/download.htm>.

W4 - NETBIOS - condivisioni Windows di rete non protette

W4.1 Descrizione:

Il protocollo *Server Message Block* (SMB), altrimenti noto come *Common Internet File System* (CIFS), abilita la condivisione dei file in rete. Una configurazione errata può esporre file critici di sistema o dare accesso completo al file system a qualsiasi malintenzionato collegato ad Internet. Molti utenti, con l'intenzione di rendere più comodo il lavoro di colleghi o ricercatori esterni, abilitano l'accesso al disco rigido del computer in lettura e in scrittura, aprendo inconsapevolmente il proprio sistema agli hacker. Gli amministratori di un centro informatico governativo dedicato allo sviluppo di software per la pianificazione delle missioni, per facilitare l'accesso ai propri file da parte del personale di altre agenzie, ne avevano abilitato la lettura a chiunque. Nel giro di due giorni gli aggressori scoprirono le condivisioni dei file aperte e si impossessarono del software per la pianificazione delle missioni.

L'abilitazione della condivisione dei file rende le macchine Windows vulnerabili sia al furto delle informazioni, sia a certi tipi di virus a diffusione rapida. Anche i computer Macintosh e Unix sono vulnerabili agli attacchi ai file condivisi se gli utenti ne abilitano la condivisione.

La caratteristica del protocollo SMB che permette la Condivisione File di Windows può essere usata dagli aggressori per ottenere informazioni sensibili dai sistemi Windows. Attraverso una connessione

con "sessione nulla" al NetBIOS Session Service, si possono ottenere informazioni sugli Utenti e sui Gruppi (nomi utente, dati sull'ultimo accesso, policy per le password, informazioni relative al RAS), informazioni di sistema e alcune chiavi del Registro. Queste informazioni sono utili agli hacker perché li aiutano a compiere gli attacchi alle password di Windows del tipo password guessing o brute force.

W4.2 Sistemi interessati:

Sistemi Microsoft Windows NT e Windows 2000.

W4.3 Lista CVE:

[CVE-1999-0366](#), [CVE-2000-0222](#), [CVE-2000-0979](#), [CAN-1999-0518](#), [CAN-1999-0519](#),
[CAN-1999-0520](#), [CAN-1999-0621](#), [CAN-2000-1079](#)

W4.4 Come stabilire se siete vulnerabili:

Una prova veloce, gratuita e sicura della presenza della condivisione file con protocollo SMB e delle relative vulnerabilità, idonea per macchine con qualsiasi tipo di sistema operativo Windows, è disponibile presso il sito Web della Gibson Research Corporation all'indirizzo <http://grc.com/>. Cliccate sull'icona "ShieldsUP" per ottenere una valutazione completa in tempo reale. Sono disponibili istruzioni dettagliate per aiutare gli utenti di Microsoft Windows ad affrontare questo tipo di vulnerabilità. Notate che se siete connessi ad una rete nella quale l'SMB è bloccato da dispositivi intermedi, ShieldsUP vi comunicherà che non siete vulnerabili anche se, in realtà, lo siete. Questo è il caso, ad esempio, dei provider che bloccano l'SMB a livello di rete per gli utenti cable-modem. ShieldsUP vi comunicherà che non sono state trovate vulnerabilità. Tuttavia, le altre 4.000 persone circa collegate sulla vostra stessa linea possono sfruttare questa vulnerabilità.

Il Microsoft Personal Security Advisor, oltre ad informarvi del fatto che siete vulnerabili agli attacchi SMB, potrà anche risolvere il problema. Dal momento che viene eseguito in locale, i risultati sono sempre attendibili. È disponibile all'indirizzo: <http://www.microsoft.com/technet/security/tools/mpsa.asp>

W4.5 Come proteggersi:

Attuate la seguente procedura per difendervi da condivisioni non protette:

1. Se avete bisogno di condividere dati, assicuratevi che siano condivise solo le directory necessarie.
2. Per maggiore sicurezza, consentite la condivisione solo per specifici indirizzi IP, poiché i nomi dei DNS possono essere contraffatti.
3. Per i sistemi Windows (sia NT che 2000) utilizzate le autorizzazioni al file system per fare in modo che i permessi alle cartelle condivise consentano l'accesso solo agli utenti che lo richiedono.
4. Nei sistemi Windows, evitate l'enumerazione anonima di utenti, gruppi, configurazione di sistema e chiavi di registro ottenibili attraverso connessioni che utilizzano una "sessione nulla". Vedere il punto W5 per maggiori informazioni.
5. Bloccate a livello di router o di host le connessioni in ingresso al NetBIOS Session Service (tcp 139) e al Microsoft CIFS (TCP/UDP 445).
6. Prendete in considerazione la possibilità di implementare la chiave di registro RestrictAnonymous per gli host connessi ad Internet in ambienti di dominio autonomo o non trusted. Per maggiori informazioni fate riferimento alle seguenti pagine Web:
Windows NT 4.0: <http://support.microsoft.com/support/kb/articles/Q143/4/74.asp>
Windows 2000: <http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP>

W5 - Perdita di informazioni causate da connessioni che utilizzano sessioni nulle

W5.1 Descrizione:

Una connessione tramite Sessione Nulla, nota anche come Accesso anonimo, è un meccanismo che consente ad un utente anonimo di ottenere informazioni (come ad esempio nomi utente e condivisioni) attraverso la rete o di connettersi senza autenticazione. Viene utilizzato da applicazioni come explorer.exe per enumerare le condivisioni sui server remoti. Nei sistemi Windows NT e Windows 2000, molti servizi locali sono eseguiti con l'account SYSTEM, noto su Windows 2000 come *LocalSystem*. L'account SYSTEM viene utilizzato per varie operazioni critiche di sistema. Quando una macchina ha bisogno di recuperare dati di sistema da un'altra, l'account SYSTEM apre una sessione nulla su questa seconda macchina.

L'account SYSTEM possiede privilegi virtualmente illimitati e non richiede alcuna password, in modo che non ci si possa connettere come SYSTEM. A volte l'account SYSTEM ha bisogno di accedere ad informazioni presenti su altre macchine come ad esempio condivisioni disponibili, nomi utente e altre funzionalità tipiche delle Risorse di Rete. Poiché non può connettersi agli altri sistemi con UserID e password, utilizza per accedere una Sessione Nulla. Sfortunatamente anche gli aggressori possono connettersi utilizzando una Sessione Nulla.

W5.2 Sistemi interessati:

Sistemi Windows NT 4.0 e Windows 2000

W5.3 Lista CVE:

[CAN-2000-1200](#)

W5.4 Come stabilire se siete vulnerabili:

Provate a connettervi al vostro sistema con una Sessione Nulla utilizzando il seguente comando:

```
net use \\a.b.c.d\ipc$ "" /user:""  
(dove a.b.c.d rappresenta l'indirizzo IP del sistema remoto).
```

Se ricevete una risposta di "connessione non riuscita", il vostro sistema non è vulnerabile. Se non ricevete alcuna risposta significa che il comando è stato eseguito con successo e il vostro sistema è vulnerabile.

Potete anche utilizzare lo strumento "*Hunt for NT*". Si tratta di un componente dell'NT Forensic Toolkit reperibile presso <http://www.foundstone.com/>.

W5.5 Come proteggersi:

I controller di dominio per comunicare richiedono sessioni nulle. Perciò, se state lavorando in un dominio di rete, potete limitare la quantità di informazioni che può cadere in mano agli aggressori, ma non potete fermarne del tutto la perdita. Per limitare la perdita di informazioni disponibili agli aggressori nelle macchine con Windows NT 4.0, modificate la seguente chiave di registro:

```
HKLM/System/CurrentControlSet/Control/LSA/RestrictAnonymous=1
```

L'impostazione di RestrictAnonymous su 1 farà in modo che alcune informazioni siano ancora disponibili agli utenti anonimi. In Windows 2000 potete invece impostare il valore a 2. Questa azione bloccherà l'accesso degli utenti anonimi a tutte le informazioni con permessi di accesso non esplicitamente assegnati all'utente anonimo o al gruppo Tutti, il quale include anche gli utenti della sessione nulla.

Qualsiasi modifica al registro potrebbe provocare il malfunzionamento del vostro sistema. Pertanto ogni modifica dovrebbe essere prima verificata. Inoltre, bisognerebbe sempre effettuare un backup del sistema per facilitarne il ripristino. Se non avete bisogno della condivisione di file e stampa, svincolate il NetBIOS dal TCP/IP.

Fate attenzione al fatto che la configurazione di RestrictAnonymous sui controller di dominio e su altri server specifici può compromettere molte normali operazioni di rete. Per questa ragione si raccomanda di configurare questo valore solo per le macchine visibili da Internet. Tutte le altre macchine dovrebbero essere protette da un firewall configurato per bloccare NetBIOS e CIFS.

L'accesso ai controller di dominio o ad altri computer non specificamente configurati per l'accesso esterno non dovrebbe essere mai consentito agli utenti Internet. Per fermare tale accesso, bloccate le seguenti porte sul router esterno o sul firewall:

TCP e UDP dalla 135 alla 139 e 445.

W6 – Hashing debole nel SAM (LM hash):

W6.1 Descrizione:

Sebbene la maggior parte degli utenti non abbia bisogno del supporto LAN Manager, i sistemi Windows NT e 2000 memorizzano, per impostazione predefinita, l'hash delle password. Siccome LAN Manager usa uno schema di codifica molto più debole di quelli, più aggiornati, attualmente utilizzati da Microsoft, le password del LAN Manager possono essere violate in brevissimo tempo. Perfino hash avanzati di password possono essere violati in meno di un mese. Le debolezze più gravi degli hash del LAN Manager sono le seguenti:

- password troncata a 14 caratteri;
- utilizzo dello spazio come carattere di riempimento nella password per raggiungere i 14 caratteri;
- password convertita in caratteri tutti maiuscoli;
- password divisa in due blocchi di sette caratteri.

Questo significa che un programma per la determinazione delle password deve scoprire solo due password di sette caratteri, addirittura senza prendere in considerazione le lettere minuscole. Inoltre, LAN Manager è vulnerabile all'intercettazione degli hash delle password. L'intercettazione può fornire agli aggressori le password degli utenti.

W6.2 Sistemi interessati:

Computer Microsoft Windows NT e 2000

W6.3 Lista CVE:

Non applicabile.

W6.4 Come stabilire se siete vulnerabili:

Se state usando un'installazione predefinita di NT o 2000, siete vulnerabili, perché l'impostazione predefinita prevede la creazione degli hash del LAN Manager. Potete verificare direttamente sul vostro sistema (dietro permesso scritto da parte del vostro datore di lavoro) la facilità con la quale le password possono essere determinate utilizzando uno strumento per la determinazione automatica delle password (password cracking tool) come LC3 (l0phtcrack versione 3), disponibile all'indirizzo:

<http://www.atstake.com/research/lc3/download.html>

W6.5 Come proteggersi:

Ci sono due metodi per proteggersi dalla determinazione della password di *LMHash*. Il primo è quello di disabilitare l'autenticazione del LAN Manager sulla rete e di usare NTLMv2. I metodi di verifica/risposta di NTLMv2 (NT Lan Manager versione 2) eliminano la maggior parte dei difetti del Lan Manager (LM) utilizzando crittografia avanzata e meccanismi superiori di autenticazione e per la sicurezza delle sessioni.

Con Windows NT 4.0 SP4 e sistemi più recenti, incluso Windows 2000, Microsoft dà la possibilità di utilizzare in rete esclusivamente NTLMv2. La chiave del registro di sistema che controlla questa proprietà in Windows NT e 2000 è

```
HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel
```

Se impostate il suo valore su 3, la stazione di lavoro o il server presenteranno per l'autenticazione solo le credenziali del NTLMv2. Se impostate il valore a 5, ogni controller di dominio rifiuterà l'autenticazione del LM e del NTLM ed accetterà solamente quella di NTLMv2.

Se in rete avete sistemi di vecchio tipo come Windows 95, dovete pianificare con cura le modifiche. I sistemi più datati non possono utilizzare NTLMv2 con il Client di rete Microsoft. In Win 9x, il parametro è

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LMCompatibility
```

ed i valori consentiti sono 0 o 3 (con il Client del servizio directory). L'opzione più sicura è quella di eliminare i sistemi più vecchi, dal momento che non vi consentono di fornire un livello di sicurezza adeguato alle esigenze attuali di un'organizzazione.

L'articolo di Microsoft Technet "How to Disable LM Authentication on Windows NT [Q147706]" illustra in dettaglio le variazioni necessarie da apportare al registro di Windows 9x e di Windows NT/2000. "LMCompatibilityLevel and Its Effects [Q175641]" chiarisce i problemi di interoperabilità di questo parametro. Un altro articolo molto utile di Technet è "How to Enable NTLMv2 Authentication for Windows 95/98/2000/NT [Q239869]". L'articolo spiega come utilizzare il Client del servizio directory di Windows 2000 per Windows 95/98 per superare le limitazioni di compatibilità imposte da NTLMv2.

Il problema della semplice rimozione degli hash del LanMan sulla rete è che gli hash vengono ancora creati e memorizzati nel SAM o nella Active Directory. Microsoft molto recentemente ha messo a disposizione un nuovo meccanismo per disabilitare del tutto la creazione degli hash di LanMan. Nei sistemi Windows 2000, andate alla seguente chiave del Registro di sistema:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

Dal menu Modifica di RegEdt32 o di RegEdit cliccate su Nuovo, Chiave e aggiungete una chiave dal nome *NoLMHash*. Quindi chiudete l'Editor del Registro di sistema e riavviate il computer. La prossima volta che un utente modifica la sua password, il computer non creerà più gli hash di LanMan. Se questa chiave viene creata su un controller di dominio di Windows 2000, gli hash di LanMan non verranno più creati né memorizzati nella Active Directory.

In Windows XP, la medesima funzionalità può essere implementata impostando un valore nel registro di sistema:

```
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Lsa
Value: NoLMHash
Type: REG_DWORD
Data: 1
```

Questa impostazione produrrà il medesimo effetto della creazione della chiave NoLMHash in Windows 2000.

Per maggiori informazioni su questo tipo di modifiche, fate riferimento all'articolo Q299656 della Microsoft KnowledgeBase in:

<http://support.microsoft.com/support/kb/articles/q299/6/56.asp>.

Le vulnerabilità principali dei sistemi Unix (U)

U1 – Buffer overflow nei Servizi RPC:

U1.1 Descrizione:

Le chiamate di procedura remota (RPC) consentono ai programmi di un computer di eseguire programmi presenti su un altro computer. Sono molto usate per l'accesso ai servizi di rete come la condivisione dei file NFS e NIS. Diverse vulnerabilità causate da difetti nelle RPC vengono oggi intensamente sfruttate. Ci sono prove convincenti che la maggior parte degli attacchi del tipo "distributed denial of service" verificatisi durante il 1999 ed i primi mesi del 2000 siano stati eseguiti da sistemi vittime delle vulnerabilità RPC. Anche l'attacco ampiamente riuscito ai sistemi delle forze armate americane durante l'incidente Solar Sunrise ha sfruttato vulnerabilità dell' RPC riscontrate su centinaia di sistemi del Dipartimento della Difesa.

U1.2 Sistemi interessati:

La maggior parte delle versioni di Unix.

U1.3 Lista CVE:

[CVE-1999-0003](#), [CVE-1999-0693](#), [CVE-1999-0696](#), [CVE-1999-0018](#), [CVE-1999-0019](#),
[CVE-1999-0704](#), [CAN-2001-0236](#), [CVE-2000-0666](#)

U1.4 Come stabilire se siete vulnerabili:

Controllate se state utilizzando uno dei tre servizi RPC più comunemente sfruttati per gli attacchi:

- rpc.ttdbserverd
- rpc.cmsd
- rpc.statd

Questi servizi vengono generalmente sfruttati per attacchi del tipo "buffer overflow", che hanno successo poiché i programmi RPC non eseguono un controllo appropriato degli errori. Le vulnerabilità del tipo "buffer overflow" consentono agli aggressori di inviare dati che il programma non si aspetta e che, poiché il programma effettua un controllo errori non adeguato, vengono lasciati passare per essere elaborati.

U1.5 Come proteggersi:

Per proteggere i vostri sistemi dagli attacchi RPC, attuate questi accorgimenti:

1. Dove possibile, disattivate e/o rimuovete questi servizi dalle macchine raggiungibili direttamente da Internet.

2. Per le macchine dove sono necessari, installate gli ultimi aggiornamenti:

Per gli aggiornamenti software Solaris:

<http://sunsolve.sun.com>

Per il software IBM AIX

<http://techsupport.services.ibm.com/support/rs6000.support/downloads>

<http://techsupport.services.ibm.com/rs6k/fixes.html>

Per gli aggiornamenti software SGI:

<http://support.sgi.com/>

Per gli aggiornamenti Compaq (Digital Unix):

<http://www.compaq.com/support>

Per Linux:

<http://www.redhat.com/support/errata/RHSA-2000-039-02.html>

<http://www.debian.org/security/2000/20000719a>

<http://www.cert.org/advisories/CA-2000-17.html>

3. Esaminate regolarmente il database degli aggiornamenti del produttore per trovare gli ultimi aggiornamenti ed installateli subito.

4. Bloccate la porta RPC (porta 111) del router perimetrale o del firewall.

5. Bloccate le porte RPC di "loopback" 32770-32789 (TCP e UDP).

Potete trovare un documento di sintesi che riporta indicazioni specifiche su ciascuna delle tre principali vulnerabilità RPC all'indirizzo: http://www.cert.org/incident_notes/IN-99-04.html

Quanto segue fornisce informazioni su ciascuno dei servizi vulnerabili:

statd: <http://www.cert.org/advisories/CA-99-05-statd-automountd.html>

ToolTalk: <http://www.cert.org/advisories/CA-98.11.tooltalk.html>

Calendar Manager: <http://www.cert.org/advisories/CA-99-08-cmsd.html>

U2 - Vulnerabilità di sendmail

U2.1 Descrizione:

Sendmail è il programma che invia, riceve e inoltra la maggior parte della posta elettronica elaborata su computer UNIX e Linux. L'uso diffuso di *Sendmail* in Internet lo rende uno degli obiettivi principali degli aggressori. Nel corso degli anni sono stati scoperti molti difetti. Il primo bollettino emesso in assoluto dal CERT/CC nel 1988, faceva riferimento proprio ad una vulnerabilità di *Sendmail*. Una delle azioni più comuni consiste nell'invio da parte dell'aggressore di un messaggio artefatto di posta elettronica alla macchina sulla quale *Sendmail* è in esecuzione; *Sendmail* legge il messaggio e lo interpreta come un'istruzione di invio del file delle password alla macchina dell'aggressore (o a quella di un'altra vittima) dove poi le password potranno essere determinate.

U2.2 Sistemi interessati:

La maggior parte delle versioni di Unix e Linux.

U2.3 Lista CVE:

[CVE-1999-0047](#), [CVE-1999-0130](#), [CVE-1999-0131](#), [CVE-1999-0203](#), [CVE-1999-0204](#),
[CVE-1999-0206](#)

U2.4 Come stabilire se siete vulnerabili:

Sendmail ha un gran numero di vulnerabilità e deve essere regolarmente aggiornato o corretto con patch di sicurezza. Controllate se avete installato l'ultima versione e l'ultimo livello di patch per *Sendmail*; se non l'avete fatto, siete probabilmente vulnerabili.

U2.5 Come proteggersi:

Per proteggere *Sendmail* si devono compiere le seguenti operazioni:

1. Effettuate l'aggiornamento di *Sendmail* all'ultima versione e/o applicate le patch.
<http://www.cert.org/advisories/CA-97.05.sendmail.html>;
2. *Sendmail* non deve essere eseguito in modalità daemon (disabilitate l'opzione *-bd*) su macchine che non siano mail server o mail relay.

U3 – Vulnerabilità di Bind

U3.1 Descrizione:

Il pacchetto software *Berkeley Internet Name Domain* (BIND) è l'implementazione di gran lunga più utilizzata del Domain Name Service (DNS) -- il sistema attraverso il quale noi tutti identifichiamo i sistemi in Internet con un nome (ad esempio www.sans.org) senza doverne conoscere lo specifico indirizzo IP; questa caratteristica lo rende uno degli obiettivi preferiti per gli attacchi. Purtroppo, secondo un'indagine condotta verso la metà del 1999, il 50% di tutti i server DNS connessi ad Internet esegue una versione di BIND vulnerabile. In un attacco "tipo" che fu condotto contro BIND, gli aggressori cancellarono i file registro del sistema e installarono strumenti per ottenere l'accesso da amministratore. Poi compilarono e installarono utility IRC e strumenti per la scansione di rete che furono utilizzati per analizzare più di una dozzina di reti di classe-B alla ricerca di ulteriori sistemi con versioni vulnerabili di BIND. Nel giro di pochi minuti, avevano usato il sistema compromesso per attaccare centinaia di sistemi remoti, riuscendo così a comprometterne molti altri. Questo è un esempio del caos che può essere generato da un'unica vulnerabilità in un software che gestisca servizi Internet onnipresenti come i DNS. Versioni non aggiornate di Bind sono anche soggette a vulnerabilità del tipo "buffer overflow", che possono essere sfruttate dagli aggressori per ottenere accessi non autorizzati.

U3.2 Sistemi interessati:

Molti sistemi UNIX e Linux.

U3.3 Lista CVE:

[CVE-1999-0024](#), [CVE-1999-0184](#), [CVE-1999-0833](#), [CVE-1999-0009](#), [CVE-1999-0835](#),
[CVE-1999-0848](#), [CVE-1999-0849](#), [CVE-1999-0851](#), [CVE-2001-0010](#), [CVE-2001-0011](#),
[CVE-2001-0013](#)

U3.4 Come stabilire se siete vulnerabili:

Utilizzate uno scanner per la rilevazione di vulnerabilità, controllate la versione di BIND, oppure controllate manualmente i file per verificare se siano vulnerabili. Nel dubbio, peccate di prudenza e aggiornate il sistema.

U3.5 Come proteggersi:

Per difendervi dalle vulnerabilità di BIND, attuate la procedura seguente:

1. Disabilitate il BIND name daemon (chiamato "named") su tutti i sistemi che non sono autorizzati ad essere server DNS. Alcuni esperti raccomandano anche di rimuovere il software DNS.
2. Su macchine che sono autorizzate ad essere server DNS, installate gli aggiornamenti all'ultima versione e il livello di patch più recente. Seguite le indicazioni contenute nei seguenti bollettini di sicurezza:
3. Per la vulnerabilità NXT:
<http://www.cert.org/advisories/CA-99-14-bind.html>

Per le vulnerabilità QINV (Inverse Query) e NAMED:
http://www.cert.org/advisories/CA-98.05.bind_problems.html
<http://www.cert.org/summaries/CS-98.04.html>

4. Come protezione da danni causati da possibili attacchi remoti, BIND deve essere eseguito come utente senza privilegi. (Tuttavia, solamente i processi in esecuzione come root possono essere configurati per utilizzare le porte sotto la 1024 – un requisito questo per i DNS. Perciò BIND deve essere configurato in modo che cambi lo user-id dopo aver effettuato il binding con la porta).

5. Come protezione da danni causati da futuri attacchi remoti, eseguite BIND in una struttura di directory chroot(ed).
6. Disabilitate i trasferimenti di zona tranne che per gli host autorizzati.
7. Disabilitate la *ricorsione* e il *glue fetching*, per difendervi dalla contaminazione della cache del DNS.
8. Nascondete la stringa di versione.

U4 - Comandi R

U4.1 Descrizione:

Le relazioni di trust sono ampiamente usate nel mondo UNIX, particolarmente per l'amministrazione di sistema. Le aziende spesso assegnano ad un unico amministratore la responsabilità di decine o addirittura di centinaia di sistemi. Gli amministratori spesso usano relazioni di trust ed i relativi comandi r di UNIX per passare agevolmente da un sistema all'altro. I comandi r consentono l'accesso ad un sistema remoto senza bisogno di fornire una password. Invece di richiedere una combinazione username/password, la macchina remota autentica chiunque provenga da un indirizzo IP "trusted". Se un aggressore ottiene il controllo di una delle macchine presenti in una rete trusted, potrà accedere a tutte le altre macchine che hanno una relazione di trust con la macchina violata. I seguenti comandi r sono spesso utilizzati:

1. rlogin – remote login
2. rsh – remote shell
3. rcp – remote copy

U4.2 Sistemi interessati:

La maggior parte delle varianti di Unix, incluso Linux

U4.3 Lista CVE:

[CVE-1999-0046](#), [CVE-1999-0113](#), [CVE-1999-0185](#), [CAN-1999-0651](#)

U4.4 Come stabilire se siete vulnerabili:

Le relazioni di trust sono stabilite configurando due file, */etc/hosts.equiv* oppure *~/.rhosts*. Controllate la presenza di entrambi i file sui vostri sistemi Unix per determinare se sono state configurate relazioni di trust.

U4.5 Come proteggersi:

Non consentite relazioni di trust basate su IP e non utilizzate i comandi r. L'autenticazione basata sugli indirizzi IP è troppo semplice da aggirare. L'autenticazione deve basarsi su mezzi più sicuri come token o, al limite, password. Se è necessario l'impiego dei comandi r, limitatene l'accesso e controllate con estrema attenzione il perimetro della rete. Non permettete mai che il file ".rhosts" sia presente nell'account "root". Potete usare il comando Unix "find" regolarmente per cercare file ".rhosts" che potrebbero essere stati creati in altri account utente.

U5 - LPD (remote print protocol daemon)

U5.1 Descrizione:

In Unix, *in.lpd* fornisce servizi agli utenti per l'interazione con la stampante locale. LPD rimane in ascolto, in attesa di richieste, sulla porta TCP 515. I programmatori che hanno sviluppato il codice che trasferisce i lavori di stampa da una macchina all'altra hanno commesso un errore che genera una vulnerabilità di

tipo "buffer overflow". Se al daemon vengono assegnati troppi lavori in un breve intervallo di tempo, esso si blocca o esegue del codice arbitrario con privilegi elevati.

U5.2 Sistemi interessati:

Sono interessati i seguenti sistemi:

- Solaris 2.6 per SPARC;
- Solaris 2.6 x86;
- Solaris 7 per SPARC;
- Solaris 7 x86;
- Solaris 8 per SPARC;
- Solaris 8 x86;
- La maggior parte delle varianti di Linux.

U5.3 Lista CVE:

[CVE-1999-0366](#), [CVE-2000-0222](#), [CVE-2000-0979](#), [CAN-1999-0518](#), [CAN-2001-0519](#),
[CAN-2001-0520](#), [CAN-1999-0621](#), [CAN-2000-1079](#)

U5.4 Come stabilire se siete vulnerabili:

Potete analizzare il vostro sistema con uno scanner per il rilevamento delle vulnerabilità oppure potete effettuare un controllo manuale. Il modo più semplice per eseguire un controllo manuale è di verificare se LPD è in esecuzione sul vostro sistema e quindi di controllarne il numero della versione.

Se avete installato una delle versioni vulnerabili del software, e se non avete applicato alcuna patch, allora siete vulnerabili.

U5.5 Come proteggersi:

Sun ha pubblicato sull'argomento il Sun Security Bulletin #00206 del 30 agosto 2001 con informazioni dettagliate riguardanti la patch. Il bollettino è disponibile presso: <http://sunsolve.sun.com/security>. L'Advisory CERT per questo argomento può essere trovato presso: <http://www.cert.org/advisories/CA-2001-15.html>

Una patch per Linux è reperibile presso <http://redhat.com/support/errata/RHSA-2001-077.html>

Altre modi per difendersi da attacchi che sfruttino questa vulnerabilità sono:

1. Disabilitare il servizio di stampa in */etc/inetd.conf* se il controllo remoto dei processi di stampa non è necessario.
2. Abilitare il **noexec_user_stack**, configurabile aggiungendo le seguenti righe al file */etc/system*, e riavviare:
 - set noexec_user_stack = 1
 - set noexec_user_stack_log = 1
3. Bloccare l'accesso alla porta di rete 515/tcp
4. Installare i [tcpwrappers](#), che fanno parte del pacchetto **tcpd-7.6** e possono essere prelevati da: <http://www.sun.com/solaris/freeware.html#cd>

U6 – *sadmind* e *mountd*

U6.1 Descrizione:

Sadmind permette l'accesso all'amministrazione remota dei sistemi Solaris, fornendo all'utente un'interfaccia grafica per le funzioni di amministrazione del sistema. *Mountd* controlla e stabilisce l'accesso ai *mount* del NFS sugli host UNIX. I "buffer overflow" in queste applicazioni, causati da errori di programmazione commessi dagli sviluppatori del software, possono essere sfruttati dagli aggressori per ottenere il controllo con privilegi di root.

Nota: questo oggetto costituisce un caso particolare di U.1 Buffer overflow nei Servizi RPC. Dato che il caso si verifica spesso, i nostri collaboratori lo considerano di importanza tale da essere trattato come elemento indipendente.

U6.2 Sistemi interessati:

Varie versioni di Unix.

U6.3 Lista CVE:

[CVE-1999-0977](#), [CVE-1999-0002](#), [CVE-1999-0493](#), [CVE-1999-0210](#)

U6.4 Come stabilire se siete vulnerabili:

Utilizzate uno scanner per la rilevazione delle vulnerabilità per verificare se questi servizi sono in esecuzione e se sono vulnerabili.

U6.5 Come proteggersi:

Le seguenti azioni vi proteggeranno dalle vulnerabilità NFS, inclusi *sadmind* e *mountd*:

1. Dove possibile, disattivate e/o rimuovete *sadmind* e *mountd* sulle macchine raggiungibili direttamente da Internet.
2. Installate le patch più recenti:
 - Patch per software Solaris:
<http://sunsolve.sun.com>
 - Per software IBM AIX
<http://techsupport.services.ibm.com/support/rs6000.support/downloads>
<http://techsupport.services.ibm.com/rs6k/fixes.html>
 - Patch per software SGI:
<http://support.sgi.com/>
 - Patch per Compaq (Digital Unix):
<http://www.compaq.com/support>
3. Usate liste di esportazione basate su *host/ip*;
4. Configurate l'esportazione dei file system in sola-lettura oppure senza *suid* dove possibile;
5. Utilizzate *nfsbug* per effettuare una scansione per la rilevazione delle vulnerabilità.

Ulteriori informazioni possono essere reperite presso:

<http://www.cert.org/advisories/CA-99-16-sadmind.html>
<http://www.cert.org/advisories/CA-98.12.mountd.html>

U7 - Stringhe SNMP predefinite

U7.1 Descrizione:

L'SNMP (Simple Network Management Protocol) è ampiamente utilizzato dagli amministratori di rete per controllare e amministrare tutti i tipi di dispositivi connessi alla rete, dai router alle stampanti e ai computer. SNMP utilizza una "community string" non cifrata come unica procedura di autenticazione. La mancanza di cifratura è già di per sé un male; a ciò si aggiunge il fatto che la community string predefinita usata dalla grande maggioranza dei dispositivi SNMP è "pubblica", e solo pochi produttori "esperti" di dispositivi di rete la modificano in "privata" per il trattamento di informazioni più sensibili. Gli aggressori possono sfruttare la vulnerabilità di SNMP per riconfigurare o per spegnere i dispositivi da remoto. Lo sniffing del traffico SNMP può rivelare molti dettagli relativi alla struttura della vostra rete e ai dispositivi ad essa collegati. Gli intrusi utilizzano queste informazioni per scegliere gli obiettivi e per pianificare gli attacchi.

Nota: l' SNMP non è un'esclusiva di Unix. Il motivo per il quale viene elencato sotto la sezione relativa a Unix sta nel fatto che i nostri collaboratori hanno riscontrato che la maggioranza degli attacchi di questo tipo avviene su sistemi Unix ed è causata da configurazioni SNMP insufficienti. Non è stato visto come un problema rilevante sui sistemi Windows.

U7.2 Sistemi interessati:

Tutti i sistemi UNIX e i dispositivi di rete.

U7.3 Lista CVE:

[CAN-1999-0517](#), [CAN-1999-0516](#), [CAN-1999-0254](#), [CAN-1999-0186](#)

U7.4 Come stabilire se siete vulnerabili:

Controllate se l'SNMP è in esecuzione sui vostri dispositivi. In caso positivo, controllate i file di configurazione per determinare la presenza delle vulnerabilità comuni:

- Community name SNMP predefiniti o vuoti;
- Community name SNMP che possono essere facilmente individuati;
- Community string SNMP nascoste.

U7.5 Come proteggersi:

Queste operazioni vi aiuteranno a difendervi dalle vulnerabilità di SNMP:

1. Se non avete necessità assoluta di utilizzare l'SNMP, disabilitatelo.
2. Se dovete usare l'SNMP, utilizzate per i community name la stessa policy delle password. Assicuratevi che essi siano difficili da indovinare o da determinare, e che siano modificati periodicamente.
3. Convalidate e controllate i community name utilizzando *snmpwalk*. Ulteriori informazioni possono essere trovate in: <http://www.zend.com/manual/function.snmpwalk.php>.
4. Filtrate SNMP (Porta 161/UDP) a livello di router perimetrale o di firewall a meno che non sia assolutamente necessario effettuare il polling o gestire i dispositivi dall'esterno della rete locale.
5. Dove possibile impostate le MIB in sola-lettura. Ulteriori informazioni possono essere trovate in: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm#xtocid210315.

Appendice A – Porte generalmente vulnerabili

In questa sezione, abbiamo elencato le porte che sono generalmente esaminate e attaccate. Il blocco di queste porte rappresenta il requisito minimo per la sicurezza perimetrale, non una lista esaustiva delle specifiche per il firewall. Una regola di gran lunga migliore sarebbe quella di bloccare tutte le porte inutilizzate. Comunque, anche se ritenete che queste porte siano bloccate, dovete sempre controllarle attivamente per scoprire eventuali tentativi d'intrusione. Un ultimo avvertimento è doveroso: il blocco di alcune delle porte elencate può disabilitare servizi necessari. Prima di implementare queste raccomandazioni, consideratene i potenziali effetti.

Tenete presente che il blocco di queste porte non rappresenta un sostituto alle soluzioni di sicurezza globali. Se le porte non sono state rese sicure in maniera adeguata su ogni sistema host della vostra organizzazione, un aggressore che ha ottenuto l'accesso alla vostra rete con altri mezzi (un modem telefonico, un trojan allegato ad un'e-mail o un complice interno all'organizzazione, per esempio) può sfruttare dette porte anche se sono bloccate.

1. Servizi di login-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin e altri (da 512/tcp a 514/tcp);
2. RPC e NFS-- Portmap/rpcbind (111/tcp e 111/udp), NFS (2049/tcp e 2049/udp), lockd (4045/tcp e 4045/udp);
3. NetBIOS in Windows NT -- 135 (tcp e udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – le prime porte più la 445(tcp e udp);
4. X Windows -- da 6000/tcp a 6255/tcp;
5. Naming Services-- DNS (53/udp) per tutte le macchine che non sono server DNS, trasferimenti di zona DNS (53/tcp) eccezion fatta per le external secondaries, LDAP (389/tcp e 389/udp);
6. Mail-- SMTP (25/tcp) per tutte le macchine che non siano relay di posta esterni, POP (109/tcp e 110/tcp), IMAP (143/tcp);
7. Web-- HTTP (80/tcp) e SSL (443/tcp) eccezion fatta per i server Web esterni, e potreste anche bloccare le comuni porte HTTP più significative (8000/tcp, 8080/tcp, 8888/tcp, ecc.);
8. "Small Services"-- porte al di sotto di 20/tcp e 20/udp, time (37/tcp e 37/udp);
9. Varie-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp e 161/udp, 162/tcp e 162/udp), BGP (179/tcp), SOCKS (1080/tcp);
10. ICMP -- bloccate le echo request in entrata (ping e traceroute di Windows), blocco delle echo reply in uscita, time exceeded e messaggi destination unreachable **eccezion fatta per i** messaggi "packet too big" (type 3, code 4). (Questo suggerimento suppone che vogliate rinunciare all'uso classico dell'echo request ICMP al fine di bloccarne alcuni noti utilizzi illeciti).

In aggiunta a queste porte, bloccate gli indirizzi "spoofed" -- pacchetti in arrivo dall'esterno della vostra azienda che hanno come sorgente indirizzi interni, indirizzi privati (RFC1918 e rete 127) e riservati IANA. Bloccate anche i pacchetti instradati alla sorgente o i pacchetti con il campo delle opzioni IP impostato.

Appendice B – Gli esperti che ci hanno aiutato a creare *Le dieci e Le venti vulnerabilità più critiche per la sicurezza in Internet.*

Phil Benchoff, Virginia Tech CIRT
Tina Bird, Counterpane Internet Security Inc.
Matt Bishop, University of California Davis
Chris Brenton, Dartmouth Inst. for Security Studies
Lee Brotzman, NASIRC Allied Technology Group Inc.
Steve Christey, MITRE
Rob Clyde, Symantec
Eric Cole, SANS Institute
Scott Conti, University of Massachusetts
Kelly Cooper, Genuity
Igor Gashinsky, NetSec Inc.
Bill Hancock, Exodus Communications
Shawn Hernan, CERT Coordination Center
Bill Hill, MITRE
Ron Jarrell, Virginia Tech CIRT
Christopher Klaus, Internet Security Systems
Valdis Kletnieks, Virginia Tech CIRT
Clint Kreitner, Center for Internet Security
Jimmy Kuo, Network Associates Inc.
Scott Lawler, Veridian
Jim Magdych, Network Associates Inc.
Dave Mann, BindView
Randy Marchany, Virginia Tech
Mark Martinec "Jozef Stefan" Institute
William McConnell, Trend Consulting Services
Peter Mell, National Institutes of Standards and Technology
Larry Merritt, National Security Agency
Mudge, @stake
Tim Mullen, AnchorIS.com
Ron Nguyen, Ernst & Young
David Nolan, Arch Paging
Stephen Northcutt, SANS Institute
Alan Paller, SANS Institute
Ross Patel, ViaCode Ltd and Afentis Security Team
Hal Pomeranz, Deer Run Associates
Chris Prorise, Foundstone Inc.
Jim Ransome
RAZOR Research - BindView Development
Martin Roesch, Snort
Vince Rowe, FBI, NIPC
Marcus Sachs, JTF-CNO US Department of Defense
Tony Sager, National Security Agency
Bruce Schneier, Counterpane Internet Security Inc.
Gene Schultz, Lawrence Berkeley Laboratory
Greg Shipley, Neohapsis
Derek Simmel, Carnegie Mellon University
Ed Skoudis, Predictive Systems
Gene Spafford, Purdue University CERIAS
Lance Spitzner, Sun Microsystems, GESS Team

Wayne Stenson, Honeywell
Jeff Stutzman
Frank Swift
Bob Todd, Advanced Research Corporation
Jeff Tricoli, FBI NIPC
Viriya Upatising, Loxley Information Services Co.
Laurie Zirkle, Virginia Tech CIRT

Appendice C: Versione italiana

La versione italiana de "Le venti vulnerabilità più critiche per la sicurezza in Internet" è stata curata dal Centro Ricerche Data Security.

Data Security Srl
Centro Ricerche

Corso Vittorio Emanuele 20 - Palazzo Concordia
33170 Pordenone
Telefono +39 0434 247206 - Fax +39 0434 26840
<http://www.datasecurity.it>

Data Security - Milano

Viale Corsica 7
20133 Milano
Telefono +39 02 454421
Fax +39 02 45442501