14.46 20/03/98
•Vulnerabilità WU-FTPD
•Accesso senza privilegi all'NFS
•Mappatura delle porte esportabili
•File di accesso al NIS password
•Accesso al REXD ("remote execution deamon")
•La vulnerabilità del "sendmail"
•Accesso ai file TFTP (Trivial File Transfert Protocol)
•Accesso a "shell" remote
•Accesso X server
•Home directory dell'ftp scrivibile

Vulnerabilità WU-FTPD

1.Sommario: accesso "root" verso il "wuarchive FTPD server".
2.Impatto: accesso remoto "root" al sistema non autorizzato.
3.Scenario: il wuarchive FTPD deamon (o WU-FTPD) è una versione altamente modificata della versione di FTP che provvede a " extra logging", a limitare il supporto ai comandi remoti e ad altre caratteristiche dello standard BSD dell'FTPD. Il codice addizionale aggiunge una notevole complessità, e moltiplica i significativi "bachi" ("bugs") software che erano già stati individuati per la versione FTPD.
4.Problemi: c'è una condizione di corsa critica nel codice, che origina un bug situato nel comando "exec", che permette a tutti (locali o remoti) l'accesso root sull'host che sta eseguendo il vulnerabile FTPD deamon. Al riguardo dell'anonymous FTP c'è da dire che non è possibile sfruttare tale vulnerabilità.
5.Conclusioni:
•- non usare le versioni estesa e modificata dell'FTPD deamons senza che sia strettamente necessario (cercare codice più stabile e sicuro).
•- promuovere il passaggio alla più recente versione del WU-FTPD; questa può essere trovata nel sito "wuarchive ftp site" all'indirizzo ftp://wuarchive.wustl.edu/packages/wuarchive-ftpd
•- restringere l'accesso FTP usando un TCP wrapper
6.Vedere anche:
1.- Cert Advisory 93:06 all'indirizzo ftp://ftp.cert.org/pub/cert_advisories/CA-93:06.wuarchive.ftpd.vulnerability.
2.- Cert Advisory 94:07 all'indirizzo ftp://ftp.cert.org/pub/cert_advisories/CA-94:07.wuarchive.ftpd.trojan.horse.

Accesso senza privilegi all'NFS

1.Sommario: il server NFS esegue le richieste di un programma utente senza i privilegi adeguati. 2.Impatto: un utente malefico può eseguire l'accesso al file NFS al posto di un altro utente. 3.Scenario: quando un "NFS clien host" vuole l'accesso ad un file o ad una directory remota, il proprio sistema operativo manda una richiesta all' NFS server. La richiesta specifica, tra l'altro, un identificatore di file, l'operazione da effettuare (lettura, scrittura, cambio dei permessi, ...) e l'identità dell'utente di cui ha preso il posto. Normalmente, l'identità

dell'utente è specificata
con il numero di utente e il numero di gruppo (ids) UNIX. Con questo schema, anche chiamato
AUTH_UNIX, il server, semplicemente, crede a quello che gli spedisce il client.
4.Problemi: la richiesta NFS non è altro che un messaggio di rete. Alcuni utenti possono eseguire un
programma che genera delle richieste NFS arbitrarie. Molti programmi sono stati disponibili per
diversi anni, e per scriverli non era necessaria una particolare attitudine alla
programmazione.
Quando l'NFS server accetta la richiesta con l'autenticazione AUTH_UNIX dal programma utente non
privilegiato, un utente malefico può eseguire la richieste di accesso ai file al
posto dell'altro
utente. Il motivo è che con una autenticazione AUTH_UNIX, l'identità dell'utente non è altro che
pochi numeri di utente e di gruppo ID in un messaggio di rete.
5.Conclusioni: è importante evitare la autenticazione AUTH_UNIX ed usare qualcosa che richiami la
crittografia. Per esempio, l'NFS è reso sicuro con il DES o le credenziali KERBEROS.
Sfortunatamente, molte implementazioni dell'NFS supportano solo le autenticazioni AUTH_UNIX.
Una soluzione parziale, ma più comune, a questo problema è riconfigurare l'NFS server, e quando
possibile, montare il deamon, per accettare le richieste solo dai programmi di
sistema con i
privilegi adatti (come UNIX kernels) e rifiutare le richieste che non hanno tali privilegi. Ciò si
applica in questo modo:
•- l'amministatore del sistema SunOS 4 deve modificare il file rpc.mountd (senza l'opzione -n) inserendo la seguente riga: < echo "nfs_portmon/W1" | adb -w /vmunix /dev/kmen >;
•- l'amministatore del sistema SunOS 5 deve modificare il file /etc/system inserendo la seguente riga: < set nfs:nfs_portmon = 1 >;
•- per altri sistemi, il comando mountd può avere opzioni differenti, e la variabile del kernel può essere chiamata nfsportmon o qualcosa di simile.
6.NOTA: il rifiuto della richiesta NFS per un programma utente non privilegiato non protegge il server contro superutenti malefici o contro maliziosi programmi di PC. 7.Altri tipi:
•- Utilizzare, dove serve, file di sistema esportati in sola lettura.
•- Bloccare le porte 2049 (NFS) e 111 (portmap) sui routers.

Mappatura delle porte esportabili

1.Sommario: NFS esporta attraverso il "portmapper". 2.Impatto: NFS esporta delle restrizioni che possono essere saltate. 3.Scenario: in modo da ottimizzare le operazioni attraverso il protocollo NFS, un client host manda
una richiesta di NFS all'NFS server deamon con:
•- un NFS file handle che specifica l'obiettivo delle operazioni,
•- le operazioni (visione, lettura, scrittura, cambio dei permessi),
•- l'utente a cui la richiesta e mandata.
4.Quando un NFS client host vuole l'accesso ad un file system remoto per la prima volta, questo, per prima cosa, deve ottenere un NFS file handle (file di
inizializzazione). Ultimata tale fase, il client host manda una richiesta di
mount al server's mount deamon. Tale server verifica che il client host abbia i
permessi per accedere al file system. Quando il mount deamon gli garantisce l'accesso allora manda un (directory) file di inizializzazione di ritorno all'NFS
client. 5.Problemi: Per ragioni di efficienza, la gran parte degli NFS export
impongono delle restrizioni attuate dal mount deamon. Le operazioni di accesso a file individuali sono controllate dall'NFS deamon, e l'origine di

molte richieste è esaminata solo in casi speciali come l'accesso remoto di un superutente. Invece di dialogare direttamente con il mount deamon, un NFS client malefico può chiedere al "server's portmapper deamon" di inoltrare la richiesta al mount deamon. Quando il mount deamon riceve la richiesta dal portmapper, il mount deamon crederà che la richesta venga dal file server, e non dal client malefico. Quando il file server esporta il file system ad esso (per esempio, perchè il server è un membro di un netgroup) il mount deamon assegna l'accesso e replica con un file handle. Il portmapper inoltra gli handle al client malefico. Da adesso in poi, il client può dialogare direttamente con il "server's NFS deamon" per accedere alla directory e ai file interni.
6.Conclusioni: eseguendo un portmapper (o un programma rpcbind nel caso di System V.4) che non fa direttamente mount ... 7.Vedere anche:
1.- Cert Advisory 94:15 all'indirizzo ftp://ftp.cert.org/pub/cert_advisories/CA-94:15.NFS.Vulnerabilities
8.Altri tipi:
•- Utilizzare, dove serve, file di sistema esportati in sola lettura.
•- Bloccare le porte 2049 (NFS) e 111 (portmap) sui routers.

File di accesso al NIS password

1.Sommario: file di accesso al NIS password di arbitrari hosts.
2.Impatto: prevede delle password automatiche per limitare gli attacchi.
3.Scenario: il NIS ("network information server") implementa un accesso di rete a campo largo per visualizzare le informazioni amministrative. Vediamo cosa contiene un esempio di archivio (chiamato anche NIS maps) che è mostrato tramite NIS:
•- il file di password che descrive quale utente ha accesso al sistema,
•- la tabella con i nomi e gli indirizzi degli hosts sulla rete,
•- "electronic mail aliases".
4.Gli archivi NIS sono organizzati in domini. Un "NIS server" può soddisfare le richieste di multipli "NIS domain". Per soddisfare una domanda, un client manda una richiesta ad un NIS server e specifica:
•- un dominio di nomi del NIS ,
•- il nome dell'archivio (NIS map) che deve essere cercato,
•- la chiave di ricerca.
5.Problemi: molte implementazioni del NIS non forniscono un controllo di accesso; ne consegue che tutti gli hosts che chiederanno informazioni riceveranno anche una risposta. Per soddisfare una domanda bisogna che il client conosca il "server's NIS domain name". Spesso questo nome è facilmente individuabile, o altrimenti può essere ottenuto tramite il "bootparam network service". Quando la rete locale è accessibile da altre reti, un intruso "remoto" può raccogliere informazioni riguardo al file di password ed eseguire un programma che possa catturare la password. Molte persone hanno dimostrato che in genere vengono scelte delle password di facile individuazione. Diversi rivenditori hanno aggiunto dei controlli di accesso alla loro implementazione di "ypserv".
6.Altri tipi:
•- Bloccare la porta 111 (portmap) sul gateway di rete. Questo rende gli attacchi sul "NIS and NFS mount deamons" molto difficili.
•- Va attuata una politica di scelta delle password utilizzando un file alternativo al file "passwd", per esempio "anlpasswd".

Accesso al REXD ("remote execution deamon")

1.Sommario: accesso remoto REXD da un arbitrario host.
2.Impatto: un intruso remoto può eseguire comandi come un normale utente.
3.Scenario: il servizio REXD e il programma client "on" implementano una esecuzione remota dei comandi tramite la rete. La sua estensione possibile, il completo ambiente client, è con l'inclusione delle directory di lavoro e

**delle
variabili d'ambiente.
4.Problemi: una richiesta per l'esecuzione di un comando remoto contiene, tra
gli altri, i comandi da eseguire, un utente, un gruppo "id". Normalmente, il
sever REXD crede a tutto quello che il client gli spedisce. Un intruso può esplorare il servizio per eseguire dei comandi come qualsiasi utente (eccetto
root). Il tipico server REXD non ha protezione contro abusi di tal genere: la
gran parte delle sue implementazioni non ha controlli di accesso nè richiede
che il client utilizzi una porta di rete privilegiata.
5.Conclusioni:
•- disabilitare il servizio REXD.
•- alcune realizzazioni del REXD possono essere configurate per usare un protocollo più sicuro.**

La vulnerabilità del "sendmail"

**1.Sommario: vulnerabilità del sendmail assortite.
2.Problemi: annotazione: questo testo fa riferimento al Cert Advisory CA-95:05 del 22 febbraio 1995.
3.Con quasi tutte le versioni del "sendmail" che erano state realizzate prima
del febbraio 1995, un utente malefico poteva guadagnare dei privilegi non autorizzati su un sistema tramite lo sfruttamento dei "newlines" negli argomenti da linea di comando o nel proprio ambiente di processo. Per poter sfruttare questo problema,l'intruso deve avere accesso ad un "account" sul tuo
sistema. In più la versione pre-8.6.10 del "sendmail" che supporta IDENT (RFC 1413) funzionalmente ha un problema che potrebbe permettere ad un intruso di guadagnare un accesso remoto non autorizzato sul sistema (senza avere accesso ad alcun account sul sistema).
4.Conclusioni:
•- sendmail va sostituito con una versione più recente, che è possibile ad esempio reperire al seguente indirizzo ftp.cs.berkeley.edu:/ucb/sendmail
•- consultare il Cert Advisory CA-95:05 all'indirizzo ftp://ftp.cert.org/pub/cert_advisories/CA-95:05.sendmail.vulnerabilities per
maggiori informazioni.**

Accesso ai file TFTP (Trivial File Transfert Protocol)

**1.Sommario: accesso ai file tramite il servizio TFTP.
2.Impatto: accesso remoto non autorizzato al sistema o ai file degli utenti.
3.Scenario: il servizio TFTP realizza un accesso remoto ai file, senza chiedere la password. Questo servizio viene usato per l'inizializzazione dei
sistemi senza disco ("diskless computer"), di X terminals, o di altri hardware
dedicati.
4.Problemi: quando il TFTP deamon non limita l'accesso a file o host specifici, un intruso ("remote intruder") potrebbe usare tale servizio per ottenere una copia del file delle password o una copia di alcuni file utente, o
potrebbe anche operare una sovrascrittura remota di alcuni file.
5.Conclusioni:
•- restringere l'accesso TFTP limitandolo solo ad un sottoalbero del tuo sistema.
•- quando non è possibile eseguire la seguente restrizione di accesso, e auspicabile tentare una ulteriore restrizione utilizzando un "tcp wrapper".**

Accesso a "shell" remote.

**1.Sommario: accesso "remote shell/remote login" da un host arbitrario.
2.Impatto: attraverso la rete la macchina può essere catturata da un**

(super)user malefico.
3.Problemi: quando il servizio "remote shell/remote login" si fida di tutti gli
hosts della rete, un superuser malefico di un qualsiasi host arbitrario può guadagnare l'accesso di ogni utente del sistema (eccetto forse l'utente root).
Una volta dentro, egli può copiare i programmi di sistema o i file di configurazione (come il password file) e quindi prendere possesso della macchina. In più, ci sono dei particolari "accounts" di tipo "guest" (ospite) o
amministrativo che non possono avere passwords di protezione: questi permettono a chiunque un login remoto come utente facendogli guadagnare l'accesso all'host.
4.Conclusioni: rimuovere la "carta di accesso" (+) dal file /etc/host.equiv.
Stai molto attento a come utilizzare la caratteristica netgroup (-@group), dato
che ci sono diverse implementazioni non corrette. Cancella o disabilita ogni
accounts senza password dal tuo sistema o dal NIS password file.
5.Altri tipi: - stabilisci gli accounts di sistema come bin e come deamon per
le shell non funzionali (come /bin/false) e inseriscili nel file /etc/ftpusers così
non potranno usare ftp.

Accesso X server

1.Sommario: accesso X server da un host arbitrario.
2.Impatto: un intruso lontano (remote intruder) può controllare la tastiera, il
mouse e lo schermo.
3.Scenario: il sistema X Window impiega un ambiente dove le applicazioni usano la rete interattivamente attraverso il workstation's display dell'utente, la
tastiera e il mouse. Ci sono due classi di programmi:
•- l'X server: il programma che dirige il workstation's display dell'utente e gli
ingressi delle periferiche.
•- l'X client: le applicazioni che vengono eseguite sulla workstation dell'utente o altrimenti sulla rete.
4.Problemi: quando l'X server permette l'accesso ad arbitrari hosts sulla rete,
un intruso (remote intruder) può connettersi all'X server e :
•- leggere ciò che viene digitato sulla tastiera dall'utente, inclusa la password
che utilizza;
•- leggere qualsiasi cosa manda sullo schermo;
•- scrivere arbitrarie informazioni sullo schermo;
•- aprire o chiudere determinate applicazioni;
•- prendere il controllo della sessione dell'utente.
5.Conclusioni: rimuovere in tutti i casi il comando "xhosts +" (nel file di sistema "Xsession", nel file utente ".xsession" e nelle altre applicazioni o
shell script che usano il sistema X window) 6.Altri tipi:
•- utilizzare il meccanismo "X magic cookie" o qualcosa di equivalente. Quando vi collegate sotto il controllo di xdm, potete attivare l'autenticazione
editando il file "xdm-config" e impostando l'attributo "the DisplayManager*authorize" a vero.
•- quando si assegna l'accesso allo schermo da un'altra macchina è preferibile
utilizzare il comando "xauth" rispetto al comando "xhost".

Home directory dell'ftp scrivibile

1.Sommario: la home directory dell'ftp è scrivibile per un utente anonimo.
2.Impatto: esecuzioni di comandi remoti, sostituzione di file remoti.
3.Problemi: quando la home directory dell'ftp di un host UNIX è scrivibile, un intruso può modificare i file ".rhosts" o ".forward" per guadagnare

l'accesso al sistema o può essere in grado di sostituire tali file. Quando un PC (DOS o MAC) permette l'accesso in scrittura ai file di sistema per l'utente anonimo, un intruso può essere capace di sostituire programmi arbitrari, con programmi da lui stesso modificati in modo da fargli ottenere l'accesso, o può sostituire dei file di configurazione, oppure può mettere in crisi il file system riempiendolo.

4.Conclusioni (UNIX):

•- rendere sicura la FTP home directory, e tutti i file system e le directory sotto di essa, assegnandogli "root" come proprietario.

•- assicurarsi che essi non siano scrivibili dall'anonimo utente. Una regola, nessun file o directory deve avere come proprietario ftp.

5.Altri tipi:

•- modificare la login shell dell'ftp account in /bin/false.

•- CERT/CC Anonymous FTP configuration guidelines.

Indicazioni.

Per avere delle informazioni più dettagliate per la maggior parte di queste metodologie di attacco sarebbe auspicabile consultare il documento "Improving the Security of Your Site by Breacking Into it" che si trova all'indirizzo ftp://ftp.switch.ch/mirror/security, mentre per maggiori dettagli sulle carenze della sicurezza si può visitare il sito ftp://ftp.cert.org/pub/