Vulnerabilità Host

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.32.101
MAC Address:	08:00:27:F4:08:97
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Approfondimento tre minacce di livello alto

192.168.32.101

136769 – Servizio ISC BIND Downgrade / Ripercussioni DoS

Sinossi: Il server dei nomi remoto è interessato dalle vulnerabilità di Service Downgrade/Reflected DoS.

Descrizione: Secondo la versione segnalata, l'istanza di ISC BIND 9, in esecuzione sul server remoto è in downgrade di prestazioni e di vulnerabilità DoS. Ciò è dovuto al fatto che BIND DNS non limita un sufficientemente il numero di recuperi che possono essere eseguiti durante l'elaborazione di una risposta di riferimento.

Soluzione: Eseguire l'aggiornamento alla versione ISC BIND a cui si fa riferimento nell'advisory del fornitore.

see also:

ISC BIND DNS DOS (fonte https://securitynews.sonicwall.com/xmlpost/isc-bind-dns-dos/)

Berkeley Internet Name Domain (BIND) è la tuta di implementazione del Domain Name Service gestita dall'Internet Systems Consortium (ISC). BIND può essere utilizzato allo scopo di mantenere e rispondere alle richieste relative a informazioni autorevoli sui domini e può fungere da server dei nomi ricorsivi.Un messaggio DNS è costituito da diversi tipi di record di risorse (RR) come il tipo A e AAAA per specificare i dettagli sulle risorse e le entità DNS. Il meccanismo di estensione per DNS (EDNS0) viene utilizzato per inviare informazioni aggiuntive sulla funzionalità come Payload Size che utilizza OPT pseudo-RR. Questo pseudo RR contiene varie opzioni, una delle quali è DNS Cookie Option che viene utilizzata per fornire sicurezza per client e server contro DoS e attacchi di contraffazione. BIND è incline a DoS. La funzione process_opt() viene chiamata quando BIND riceve OPT pseudo-RR che controlla le variabili, sitbad e sitgood sono zero dopo aver ricevuto l'opzione COOKIE usando l'asserzione INSIST e quindi imposta una delle variabili su una in base al cookie ricevuto. Se incontra la seconda opzione COOKIE, porta a un errore di asserzione a causa di una delle variabili sitbad o sitgood precedentemente impostate. In questo modo BIND termina. L'utente malintenzionato remoto può sfruttare questa vulnerabilità inviando messaggi DNS predisposti che possono causare la condizione del servizio Daniel. Questa vulnerabilità interessa i seguenti prodotti: ISC BIND dalla versione 9.10.0 alla 9.10.3-P3. Il team di ricerca sulle minacce Dell SonicWALL ha studiato questa vulnerabilità e rilasciato le seguenti firme per proteggere i propri clienti:

IPS:11525 ISC BIND Cookie Option DoS

42256 – Condivisioni NFS leggibili in tutto il mondo

Sinossi: Il server remoto NFS è esposto in tutto il mondo

Descrizione: Il server NFS remoto esporta una o più condivisioni senza limitare l'accesso (in base a nome host, IP, o intervallo IP).

Soluzione: Applicare le restrizioni appropriate a tutte le condivisioni NFS.

see also:

Sicurezza e Nsf (fonte: https://tldp.org/HOWTO/NFS-HOWTO/security.html)

Questo elenco di suggerimenti e spiegazioni sulla sicurezza non renderà il tuo sito Completamente sicuro. NIENTE renderà il tuo sito completamente sicuro. Lettura di questa sezione può aiutarti a farti un'idea dei problemi di sicurezza con NFS. Questo non è una guida completa e sarà sempre in fase di cambiamenti. Se si avere suggerimenti o suggerimenti da darci si prega di inviarli al HOWTO mantenitore. Se sei su una rete senza accesso al mondo esterno (nemmeno un modem) e ti fidi di tutte le macchine interne e di tutti i tuoi utenti Questa sezione non ti sarà di alcuna utilità. Tuttavia, è nostra convinzione che Ci sono relativamente poche reti in questa situazione, quindi vorremmo suggerire leggere attentamente questa sezione per chiunque configuri NFS. Con NFS, ci sono due passaggi necessari per un client per ottenere l'accesso a File contenuto in una directory remota sul server. Il primo passo è montare accesso. L'accesso al montaggio viene raggiunto dal computer client che tenta di connettersi al server. La sicurezza per questo è fornita dal file /etc/exports. Questo file elenca i nomi o gli indirizzi IP delle macchine che sono autorizzati ad accedere a un punto di condivisione. Se l'indirizzo IP del client corrisponde a una delle voci nell'elenco di accesso, quindi sarà consentito montare. Questo non è terribilmente sicuro. Se qualcuno è in grado di falsificare o Prendendo in consegna un indirizzo attendibile, possono accedere ai tuoi punti di montaggio. A dare un esempio reale di questo tipo di "autenticazione": Questo è equivalente a qualcuno che si presenta a te e tu credi di sono chi affermano di essere perché indossano un adesivo che dice "Ciao, il mio nome è ...." Una volta che la macchina ha montato un volume, il suo Il sistema operativo avrà accesso a tutti i file sul volume (con il comando possibile eccezione di quelli di proprietà di root; vedi sotto) e accesso in scrittura anche in questi file, se il volume è stato esportato con l'opzione RW. Il secondo passo è l'accesso ai file. Questa è una funzione del normale file system controlli di accesso sul client e non una funzione specializzata di NFS. Una volta montata l'unità, le autorizzazioni utente e di gruppo sui file Determinare il controllo degli accessi. Un esempio: bob sul server viene mappato all'ID utente 9999. Bob crea un file sul server accessibile solo all'utente (l'equivalente di digitare il nome del file CHMOD 600). Un client è autorizzato a montare l'unità in cui è memorizzato il file. Sul client Mary map a UserID 9999. Ciò significa che il cliente L'utente Mary può accedere al file di Bob contrassegnato come accessibile solo da lui. Peggiora: se qualcuno è diventato superutente sulla macchina client, può diventare equalsiasi utente. NFS non sarà più saggio. Ci sono alcune misure che puoi adottare sul server per compensare il pericolo dei clienti. Ne parleremo a breve. Se pensi che le misure di sicurezza non si applichino a te, probabilmente sei sbagliato.

42873 - Suite di crittografia SSL con supporto a media potenza (SWEET32)

Sintassi: Il servizio remoto supporta l'uso di SSL cifrate di media potenza.

Descrizione: L'host remoto supporta l'uso di crittografie SSL a media potenza. Si consigliano

chiave crittografate comprese tra 64 bit e 112 bit, oppure

che si utilizzi la suite di crittografia 3DES.

Soluzione: Riconfigurare l'applicazione interessata, se possibile,

per evitare l'utilizzo di crittografie di media intensità.

see also:

Il problema SWEET32, CVe-2016-2183 (fonte: https://www.openssl.org/blog/blog/2016/08/24/sweet32/)

DES (e triple-DES) ha solo una dimensione del blocco di 64 bit, gli attacchi di compleanno sono una vera preoccupazione. Con la possibilità di eseguire Javascript in un browser, È possibile inviare abbastanza traffico per causare una collisione e quindi utilizzare tali informazioni per recuperare qualcosa come un cookie di sessione. Loro Gli esperimenti sono stati in grado di recuperare un cookie in meno di due giorni. Maggiori dettagli sono disponibili sul loro sito web. Ma il take-away è questo: triple-DES dovrebbe ora essere considerato "cattivo" come RC4. Triple-DES, che appare come "DES-CBC3" in una stringa di crittografia OpenSSL, è ancora utilizzato sul Web, e i principali browser non sono ancora disposti a completamente disabilitarlo. Se si esegue un server, è necessario disabilitare triple-DES. Questo è generalmente un problema di configurazione. Se si esegue un server obsoleto che non supporta alcun server cifrari migliori di DES o RC4, è necessario aggiornare. All'interno del team OpenSSL, abbiamo discusso su come classificare questo, utilizzando la nostrapolitica di sicurezza, e abbiamo ha deciso di valutarlo BASSO. Ciò significa che abbiamo appena inserito la correzione nel nostro Repository. Ecco cosa abbiamo fatto: per 1.0.2 e 1.0.1, abbiamo rimosso i cifrari triple-DES da "HIGH" e inserirli in "MEDIUM". Nota chenonabbiamo rimosso dalla parola chiave "DEFAULT". Per la versione 1.1.0, che prevediamo di rilasciare domani, trattare il triplo DES proprio come stiamo trattando RC4. Non è compilato da default; Devi usare "enable-weak-ssl-ciphers" come opzione di configurazione. Anche quando questi cifrari sono compilati, triple-DES è solo nel "MEDIUM" parola chiave. Inoltre, poiché si tratta di una nuova versione, l'abbiamo anche rimossa. dalla parola chiave "DEFAULT".Quando si dispone di una grande base installata, è difficile andare avanti in un certo senso che piacerà a tutti. Lasciando triple-DES in "DEFAULT" per 1.0.x e Rimuoverlo dalla versione 1.1.0 è certamente un compromesso. Speriamo che le modifiche di cui sopra abbiano senso, e Anche se non sei d'accordo e gestisci un server, puoi proteggere in modo esplicito il tuo utente attraverso la configurazione.