



Version 10.3.0-debian9_amd64

METASPLOITABLE

Report generated by Nessus™

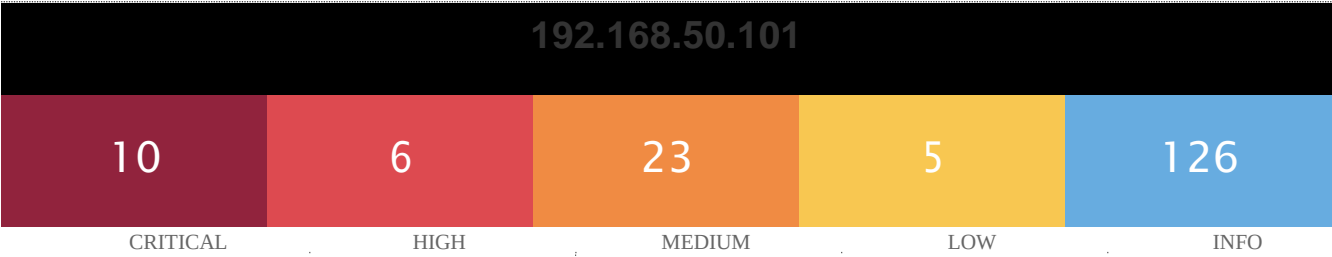
Thu, 24 Nov 2022 14:03:51 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.50.101	4
------------------------	---

Vulnerabilities by Host




Scan Information

Start time: Thu Aug 4 08:37:10 2022
End time: Thu Aug 4 09:03:51 2022

Host Information

Netbios Name: METASPL
OITABLE IP: 192.168.50.101
MAC Address: 08:00:27:52:71:A7
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

 <p>Assessed Threat Level: High</p> <p>The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk. Click on each finding to show further details along with the impacted hosts. To learn more about Tenable's VPR scoring system, see Predictive Prioritization.</p>				
VPR Severity	Name	Reasons	VPR Score ▼	Hosts
HIGH	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Social Media	8.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	No recorded events	7.4	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	No recorded events	6.3	1
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	No recorded events	6.1	1
MEDIUM	ISC BIND Service Downgrade / Reflected DoS	No recorded events	6.0	1
MEDIUM	NFS Exported Share Information Disclosure	No recorded events	5.9	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	No recorded events	5.3	1
MEDIUM	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	No recorded events	5.2	1

HIGH

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Social Media

8.4

1

Sommario:

C'è un connettore AJP vulnerabile in ascolto sull'host remoto.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +

Punteggio di impatto CVSSv3: 5,9

Scadenza codice exploit: Funzionale

Copertura del prodotto: molto alta

Intensità della minaccia: molto bassa

Recente minaccia: da 7 a 30 giorni

Fonti di minaccia: social media Host interessati (1)

Descrizione:

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server vulnerabile. Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JSP (JavaServer Pages) dannoso all'interno di una varietà di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione:

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiorna il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

Informazioni sulla vulnerabilità:

CPE: cpe:/a:apache:tomcat

Exploit disponibile: vero

Facilità di exploitare: sono disponibili exploit

Patch pubblicata: 1 marzo 2020

Vulnerabilità Pubblicato: 1 marzo 2020

Sinossi:

Le chiavi host SSH remote sono deboli.

Valutazione della priorità delle vulnerabilità

Età di vulnerabilità: 730 giorni + Punteggio di impatto CVSSv3: 5,9

Scadenza codice exploit: Funzionale

Copertura del prodotto: bassa

Intensità della minaccia: molto bassa

Minaccia recente: nessun evento registrato

Fonti di minaccia: nessun evento registrato

Host interessati (1)

Descrizione:

La chiave host SSH remota è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per impostare la decifrazione della sessione remota o impostare un uomo nel mezzo dell'attacco.

Soluzione:

Considera che tutto il materiale crittografico generato sull'host remoto sia intuibile. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Informazioni sui rischi:

Fattore di rischio: alto

Punteggio base CVSS: 7,5 su 10,0

Informazioni sui rischi:

Fattore di rischio: critico

Punteggio base CVSS: 10,0 su 10,0

Informazioni sulla vulnerabilità:

Exploit disponibile: vero

Facilità di exploit: sono disponibili exploit (core Impact)

Sinossi:

Il certificato SSL remoto utilizza una chiave debole.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +

Punteggio di impatto CVSSv3: 5,9

Scadenza codice exploit: Funzionale

Copertura del prodotto: bassa

Intensità della minaccia: molto bassa

Minaccia recente: nessun evento registrato

Fonti di minaccia: nessun evento registrato

Descrizione:

Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un packager Debian che rimuove quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un uomo nel mezzo dell'attacco.

Soluzione:

Considerare intuibile tutto il materiale crittografico generato sull'host remoto. In particolare, tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

Informazioni sui rischi:

Fattore di rischio: critico

Punteggio base CVSS: 10 su 10

Informazioni sulla vulnerabilità:

Exploit disponibile: vero

Facilità di exploit: sono disponibili exploit (con Core Impact)

Patch pubblicata: 14 maggio 2008

Vulnerabilità Pubblicato: 13 maggio 2008

MEDIUM

Samba Badlock Vulnerability

No recorded events

6.7

1

Sinossi:

Un server SMB in esecuzione sull'host remoto è interessato dalla vulnerabilità Badlock.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +

Punteggio di impatto CVSSv3: 5,9

Scadenza codice exploit: non dimostrata

Copertura del prodotto: media

Intensità della minaccia: molto bassa

Minaccia recente: nessun evento registrato

Fonti di minaccia: nessun evento registrato

Host interessati (1)

Descrizione:

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, che esiste in Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) protocolli a causa della negoziazione del livello di autenticazione improprio sui canali RPC (Remote Procedure Call). Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati di sicurezza sensibili nel database di Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione:

Esegui l'upgrade alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Informazioni sui rischi:

Fattore di rischio: medio

Punteggio base CVSS: 6,8 su 10,0

Informazioni sulla vulnerabilità

CPE: cpe:/a:samba:samba

Exploit disponibile: falso

Facilità di sfruttamento: non sono disponibili exploit noti

Patch pubblicata: 12 aprile 2016

Vulnerabilità Pubblicato: 23 marzo 2016

MEDIUM

SMTP Service STARTTLS Plaintext Command Injection

No recorded events

6.3

1

Sinossi:

Il servizio di posta remota consente l'iniezione di comandi in chiaro durante la negoziazione di un canale di comunicazione crittografato.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +

Punteggio di impatto CVSSv3: 5,5

Scadenza codice exploit: PoC

Copertura del prodotto: bassa

Intensità della minaccia: molto bassa

Minaccia recente: nessun evento registrato

Fonti di minaccia: nessun evento registrato

Host interessati (1)

Descrizione:

Il servizio SMTP remoto contiene un difetto software nella sua implementazione STARTTLS che potrebbe consentire a un utente malintenzionato remoto non autenticato di iniettare comandi durante la fase del protocollo in chiaro che verrà eseguito durante la fase del protocollo del testo cifrato. Lo sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o le credenziali SASL (Simple Authentication and Security Layer) associate.

Soluzione:

Contattare il fornitore per vedere se è disponibile un aggiornamento.

Informazioni sui rischi:

Fattore di rischio: medio

Punteggio base CVSS: 4,0 su 10,0

Informazioni sulla vulnerabilità:

Sfrutta disponibile: vero

Facilità di sfruttamento: sono disponibili exploit

Vulnerabilità Pubblicato: 7 marzo 2011

Sinossi:

Il servizio remoto supporta l'uso di crittografie SSL di livello medio.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +
Punteggio di impatto CVSSv3: 3.6
Scadenza codice exploit: Funzionale
Copertura del prodotto: alta
Intensità della minaccia: molto bassa
Minaccia recente: nessun evento registrato
Fonti di minaccia: nessun evento registrato
Host interessati (1)

Descrizione:

L'host remoto supporta l'uso di crittografie SSL che offrono una crittografia di livello medio. Nessus considera di livello medio qualsiasi crittografia che utilizzi chiavi di lunghezza pari ad almeno 64 bit e inferiori a 112 bit, oppure che utilizzi la suite di crittografia 3DES. Si noti che è notevolmente più facile aggirare la crittografia di livello medio se l'attaccante si trova sulla stessa rete fisica.

Soluzione:

Se possibile, riconfigurare l'applicazione interessata per evitare l'uso di cifrari di media intensità.

Informazioni sui rischi:

Fattore di rischio: medio
Punteggio base CVSS: 5,0 su 10,0

Informazioni sulla vulnerabilità:

Vulnerabilità Pubblicato: 24 agosto 2016

Sinossi:

Il server dei nomi remoto è interessato dalle vulnerabilità di downgrade del servizio/DoS riflesso

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +
Punteggio di impatto CVSSv3: 4
Scadenza codice exploit: Funzionale
Copertura del prodotto: bassa
Intensità della minaccia: molto bassa
Minaccia recente: nessun evento registrato
Fonti di minaccia: nessun evento registrato
Host interessati (1)

Descrizione:

Secondo la sua versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul server dei nomi remoto è interessata dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Ciò è dovuto al fatto che BIND DNS non limita a sufficienza il numero di recuperi che

possono essere eseguiti durante l'elaborazione di una risposta di riferimento. Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio del server ricorsivo o per utilizzare il server interessato come riflettore in un attacco di riflessione.

Soluzione:

Aggiornamento alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore.

Informazioni sui rischi:

Fattore di rischio: medio

Punteggio base CVSS: 5,0 su 10

Informazioni sulla vulnerabilità:

CPE: cpe:/a:isc:bind

Facilità di sfruttamento: non sono disponibili exploit noti

Patch pubblicata: 19 maggio 2020

Vulnerabilità Pubblicato: 19 maggio 2020

MEDIUM

NFS Exported Share Information Disclosure

No recorded events

5.9

1

Sinossi:

È possibile accedere alle condivisioni NFS sull'host remoto.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +

Punteggio di impatto CVSSv3: 5,9

Scadenza codice exploit: non dimostrata

Copertura del prodotto: bassa

Intensità della minaccia: molto bassa

Minaccia recente: nessun evento registrato

Fonti di minaccia: nessun evento registrato

Host interessati (1)

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttarlo per leggere (e possibilmente scrivere) file sull'host remoto.

Soluzione:

Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Informazioni sui rischi:

Fattore di rischio: critico

Punteggio base CVSS: 10.0 su 10.0

Informazioni sulla vulnerabilità:

Sfrutta disponibile: vero

Facilità di sfruttamento: sono disponibili exploit (Metasploit NFS Mount Scanner)

Vulnerabilità Pubblicato: 1 gennaio 1985

Sinossi:

È possibile ottenere informazioni sensibili dall'host remoto con servizi abilitati SSL/TLS.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +

Punteggio di impatto CVSSv3: 1.4

Scadenza codice exploit: Funzionale

Copertura del prodotto: molto alta

Intensità della minaccia: molto bassa

Minaccia recente: nessun evento registrato

Fonti di minaccia: nessun evento registrato

Host interessati (1)

Descrizione:

L'host remoto è interessato da una vulnerabilità di divulgazione di informazioni man-in-the-middle (MitM) nota come POODLE. La vulnerabilità è dovuta al modo in cui SSL 3.0 gestisce i byte di riempimento durante la decrittografia dei messaggi crittografati utilizzando i codici a blocchi in modalità Cipher Block Chaining (CBC). Gli aggressori MitM possono decrittografare un byte selezionato di un testo cifrato in soli 256 tentativi se sono in grado di forzare un'applicazione vittima a inviare ripetutamente gli stessi dati su connessioni SSL 3.0 appena create. Finché un client e un servizio supportano entrambi SSLv3, è possibile eseguire il "rollback" di una connessione su SSLv3, anche se TLSv1 o versione successiva è supportato dal client e dal servizio. Il meccanismo TLS Fallback SCSV previene gli attacchi di "rollback della versione" senza influire sui client legacy; tuttavia, può proteggere le connessioni solo quando il client e il servizio supportano il meccanismo. I siti che non possono disabilitare immediatamente SSLv3 dovrebbero abilitare questo meccanismo. Questa è una vulnerabilità nella specifica SSLv3, non in una particolare implementazione SSL. La disabilitazione di SSLv3 è l'unico modo per mitigare completamente la vulnerabilità.

Soluzione:

Disabilita SSLv3.

I servizi che devono supportare SSLv3 devono abilitare il meccanismo SCSV di fallback TLS finché SSLv3 non può essere disabilitato.

Informazioni sui rischi:

Fattore di rischio: medio

Punteggio base CVSS: 4.3

Informazioni sulla vulnerabilità:

Exploit disponibile: falso

Facilità di sfruttamento: non sono disponibili exploit noti

Vulnerabilità Pubblicato: 14 ottobre 2014

Sinossi:

L'host remoto supporta una serie di crittografie deboli.

Valutazione della priorità delle vulnerabilità:

Età di vulnerabilità: 730 giorni +
Punteggio di impatto CVSSv3: 3.7
Scadenza codice exploit: Funzionale
Copertura del prodotto: bassa
Intensità della minaccia: molto bassa
Minaccia recente: nessun evento registrato
Fonti di minaccia: nessun evento registrato
Host interessati (1)

Descrizione:

L'host remoto supporta le suite di crittografia EXPORT_RSA con chiavi inferiori o uguali a 512 bit. Un utente malintenzionato può fattorizzare un modulo RSA a 512 bit in un breve lasso di tempo. Un utente malintenzionato potrebbe essere in grado di eseguire il downgrade della sessione per utilizzare le suite di crittografia EXPORT_RSA (ad es. CVE-2015-0204). Pertanto, si consiglia di rimuovere il supporto per le suite di crittografia deboli.

Soluzione:

Riconfigurare il servizio per rimuovere il supporto per le suite di crittografia EXPORT_RSA.

Informazioni sui rischi:

Fattore di rischio: medio
Punteggio base CVSS: 4.3

Informazioni sulla vulnerabilità:

Exploit disponibile: falso
Facilità di sfruttamento: non sono disponibili exploit noti
Patch pubblicata: 8 gennaio 2015
Vulnerabilità Pubblicato: 8 gennaio 2015