REPORT Vulnerabilità Critiche

Vulnerabilità Critica: Ghostcat (CVE-2020-1938)

La vulnerabilità Ghostcat consente a un utente malintenzionato non autenticato di leggere file arbitrari dall'applicazione web e potenzialmente eseguire codice dannoso sul server, se quest'ultimo permette l'upload di file. L'attacco sfrutta una falla nel connettore AJP di Apache Tomcat, esposto di default sulla porta 8009.

Impatto:

- **Esposizione dati sensibili:** Possibile accesso non autorizzato a file di configurazione, database, credenziali, etc.
- **Compromissione del server:** Rischio di esecuzione di codice arbitrario, permettendo all'attaccante di prendere il controllo completo del sistema.

Soluzione:

- **Aggiornamento:** Aggiornare Apache Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successiva.
- **Configurazione AJP:** Configurare il connettore AJP per richiedere l'autenticazione.

Vulnerabilità Critica: Debolezza nel Generatore di Numeri Casuali di OpenSSH/OpenSSL su Debian (CVE-2008-0166)

Questa vulnerabilità riguarda i sistemi Debian e Ubuntu che utilizzano versioni di OpenSSL affette da un bug nel generatore di numeri casuali. A causa di una rimozione impropria di fonti di entropia durante il processo di packaging, le chiavi crittografiche generate su questi sistemi (incluse le chiavi SSH) sono facilmente indovinabili.

Impatto:

- **Compromissione delle comunicazioni SSH:** Un attaccante può decifrare il traffico SSH o eseguire attacchi man-in-the-middle, ottenendo l'accesso non autorizzato al sistema remoto.
- **Compromissione di altri servizi crittografici:** Anche chiavi SSL e OpenVPN potrebbero essere vulnerabili, mettendo a rischio la sicurezza di altri servizi.

Soluzione:

- **Rigenerare tutte le chiavi:** È fondamentale rigenerare tutte le chiavi crittografiche generate sul sistema interessato, incluse chiavi SSH, SSL e OpenVPN.
- **Aggiornare OpenSSL:** Assicurarsi di utilizzare una versione di OpenSSL che non sia affetta da questa vulnerabilità.

Vulnerabilità Critica: Debolezza nel Generatore di Numeri Casuali di OpenSSL su Debian (CVE-2008-0166)

Questa vulnerabilità riguarda i certificati SSL generati su sistemi Debian o Ubuntu che utilizzano versioni di OpenSSL affette da un bug nel generatore di numeri casuali. A causa di una rimozione impropria di fonti di entropia durante il processo di packaging, le chiavi private associate a questi certificati sono facilmente indovinabili.

Impatto:

- **Compromissione delle comunicazioni SSL/TLS:** Un attaccante può decifrare il traffico HTTPS o eseguire attacchi man-in-the-middle, compromettendo la riservatezza e l'integrità dei dati trasmessi.

Soluzione:

- **Rigenerare il certificato SSL:** È fondamentale rigenerare il certificato SSL/TLS sul server interessato utilizzando una versione di OpenSSL non affetta da questa vulnerabilità.

Vulnerabilità Critica: Debolezza nel Generatore di Numeri Casuali di OpenSSL su Debian (CVE-2008-0166)

Descrizione:

Un certificato SSL/TLS presente sul server remoto è stato generato su un sistema Debian o Ubuntu affetto da un bug critico nel generatore di numeri casuali di OpenSSL. Questo bug, introdotto durante il processo di packaging Debian, ha rimosso quasi tutte le fonti di entropia necessarie per generare chiavi crittograficamente sicure. Di conseguenza, la chiave privata associata al certificato è facilmente prevedibile e può essere ottenuta da un attaccante.

Impatto:

- **Compromissione della riservatezza e integrità dei dati:** Un attaccante può decifrare il traffico HTTPS protetto dal certificato vulnerabile, esponendo informazioni sensibili come credenziali di accesso, dati personali o transazioni finanziarie.
- **Attacchi Man-in-the-Middle:** L'attaccante può impersonare il server legittimo, intercettando e manipolando le comunicazioni tra il client e il server.

Soluzione:

- **Considerare compromesso tutto il materiale crittografico generato sull'host remoto.** In particolare, tutte le chiavi SSH, SSL e OpenVPN dovrebbero essere rigenerate.

Vulnerabilità: Utilizzo di protocolli SSL/TLS obsoleti (SSL 2.0 e 3.0)

Descrizione:

Il servizio remoto accetta connessioni che utilizzano i protocolli SSL 2.0 e/o SSL 3.0, entrambi considerati insicuri a causa di diverse vulnerabilità crittografiche note. Queste vulnerabilità possono consentire ad un attaccante di eseguire attacchi man-in-the-middle o decifrare le comunicazioni tra il servizio e i suoi client.

Impatto:

- **Compromissione della riservatezza:** Possibilità di intercettazione e decifrazione del traffico dati, esponendo informazioni sensibili.
- **Attacchi Man-in-the-Middle:** Possibilità di interposizione di un attaccante nella comunicazione, consentendo la manipolazione o l'alterazione dei dati scambiati.

Soluzione:

- **Disabilitare SSL 2.0 e 3.0:** Consultare la documentazione dell'applicazione per disabilitare questi protocolli obsoleti.
- **Utilizzare TLS 1.2 o superiore:** Configurare il servizio per utilizzare esclusivamente TLS 1.2 o versioni successive, assicurandosi di selezionare suite di cifratura robuste e approvate.

Vulnerabilità Critica: Backdoor in UnrealIRCd

Descrizione:

Il server IRC remoto è una versione di UnrealIRCd che contiene una backdoor. Questa backdoor consente a un utente malintenzionato di eseguire codice arbitrario sul server interessato, compromettendone la sicurezza e potenzialmente ottenendo il controllo completo del sistema.

Impatto:

- **Esecuzione di codice remoto:** Un attaccante può sfruttare la backdoor per eseguire comandi dannosi sul server, rubare dati sensibili, installare malware o compromettere ulteriormente l'infrastruttura.

Soluzione:

- **Reinstallazione del software:** Scaricare nuovamente il software da una fonte affidabile, verificare l'integrità del file utilizzando i checksum MD5 o SHA1 pubblicati e reinstallarlo.

Vulnerabilità: Password Debole su Server VNC

Il server VNC in esecuzione sul sistema remoto utilizza la password debole "password". Questa vulnerabilità consente a un utente malintenzionato non autenticato di accedere al sistema tramite VNC e assumere il controllo completo.

Impatto:

- **Accesso non autorizzato al sistema:** Un attaccante può sfruttare questa debolezza per ottenere l'accesso completo al sistema, visualizzare e controllare il desktop, installare malware, rubare dati sensibili o causare danni.

Soluzione:

- **Cambiare la password VNC:** Impostare immediatamente una password complessa e univoca per il server VNC.