Vulnerabilità modalità CBC debole protocollo SSL v3 e TLS v1

Sommario

Introduzione

In questo documento viene descritto come disabilitare i cifrari in modalità CBC (Cipher Block Chaining) su Cisco Email Security Appliance (ESA). Un controllo/analisi della sicurezza può segnalare che un'ESA presenta una vulnerabilità in modalità CBC vulnerabile per il protocollo Secure Sockets Layer (SSL) v3/Transport Layer Security (TLS) v1.

> **Attenzione**: Se si utilizza un codice precedente di AsyncOS for Email Security, si consiglia di eseguire l'aggiornamento alla versione 11.0.3 o successive. Consulta le Note di rilascio di Cisco Email Security per informazioni e versioni più recenti. Per ulteriore assistenza nell'aggiornamento o nella disabilitazione delle cifrature, aprire una richiesta di assistenza.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano su AsyncOS for Email Security (qualsiasi revisione), Cisco ESA e un'ESA virtuale.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

- La conformità allo standard PCI DSS (Payment Card Industry Data Security Standard) richiede la disabilitazione dei cifrari CBC.
- Un controllo/analisi della sicurezza ha identificato una potenziale vulnerabilità con i protocolli SSL v3/TLS v1 che utilizzano i cifrari in modalità CBC.

  Suggerimento: SSL versione 3.0 (RFC-6101) è un protocollo obsoleto e non sicuro. È presente una vulnerabilità in SSLv3 CVE-2014-3566 nota come attacco Padding Oracle On Downgraded Legacy Encryption (POODLE), ID bug Cisco CSCur27131. Si consiglia di disabilitare SSL v3 mentre si modificano i cifrari e si usa solo TLS, quindi selezionare l'opzione 3 (TLS v1). Per i dettagli completi, consultare l'ID bug Cisco CSCur27131 fornito.

I protocolli SSL v3 e TLS v1 vengono utilizzati per fornire integrità, autenticità e privacy ad altri protocolli, ad esempio HTTP e LDAP (Lightweight Directory Access Protocol). Forniscono questi servizi con l'utilizzo della crittografia per la privacy, certificati x509 per l'autenticità e funzionalità di crittografia unidirezionale per l'integrità. Per crittografare i dati, SSL e TLS possono utilizzare cifrature a blocchi, ossia algoritmi di crittografia in grado di crittografare solo un blocco fisso di dati originali su un blocco crittografato delle stesse dimensioni. Si noti che questi cifrari otterranno sempre lo stesso blocco risultante per lo stesso blocco di dati originale. Per ottenere una differenza nell'output, l'output della crittografia viene XORed con un altro blocco della stessa dimensione chiamato vettori di inizializzazione (IV). CBC utilizza un IV per il blocco iniziale e il risultato del blocco precedente per ogni blocco successivo per ottenere la differenza nell'output della crittografia a blocchi.

Nell'implementazione di SSL v3 e TLS v1, l'utilizzo della modalità CBC scelta è stato scarso in quanto l'intero traffico condivide una sessione CBC con un singolo set di IV iniziali. Gli altri IV sono, come accennato in precedenza, il risultato della crittografia dei blocchi precedenti. I successivi IV sono a disposizione degli intercettatori. Ciò consente a un utente non autorizzato di iniettare traffico arbitrario nel flusso di testo normale (da crittografare da parte del client) per verificare la propria ipotesi del testo normale che precede il blocco inserito. Se la stima degli aggressori è corretta, l'output della crittografia è lo stesso per due blocchi.

Per i dati di entropia bassi, è possibile indovinare il blocco di testo normale con un numero relativamente basso di tentativi. Ad esempio, per i dati con 1000 possibilità, il numero di tentativi può essere 500.

Requisiti

Perché l'exploit funzioni, è necessario che vengano soddisfatti diversi requisiti:

1. La connessione SSL/TLS deve utilizzare una delle cifrature di crittografia a blocchi che utilizzano le modalità CBC, ad esempio DES o AES. I canali che utilizzano cifrari di flusso come RC4 non sono soggetti a questo difetto. Un'ampia percentuale di connessioni SSL/TLS utilizza RC4.
2. La vulnerabilità può essere sfruttata solo da qualcuno che intercetta i dati sulla connessione SSL/TLS e invia attivamente nuovi dati su tale connessione. Lo sfruttamento del difetto causa l'interruzione della connessione SSL/TLS. L'autore dell'attacco deve continuare a monitorare e utilizzare le nuove connessioni fino a quando non vengono raccolti dati sufficienti per decrittografare il messaggio.
3. Poiché la connessione viene terminata ogni volta, il client SSL/TLS deve essere in grado di continuare a ristabilire il canale SSL/TLS per un periodo di tempo sufficiente a decrittografare

il messaggio.
4. L'applicazione deve inviare nuovamente gli stessi dati su ogni connessione SSL/TLS creata e il listener deve essere in grado di individuarli nel flusso di dati. Protocolli come IMAP/SSL che dispongono di un set fisso di messaggi per l'accesso soddisfano questo requisito. L'esplorazione generale del Web non lo consente.

Minaccia

La vulnerabilità CBC è una vulnerabilità di TLS v1. Questa vulnerabilità esiste dall'inizio del 2004 ed è stata risolta nelle versioni più recenti di TLS v1.1 e TLS v1.2.

Nelle versioni precedenti a AsyncOS 9.6 for Email Security, l'ESA utilizza cifrari in modalità TLS v1.0 e CBC. Con AsyncOS 9.6, l'ESA introduce TLS v1.2. Tuttavia, i cifrari in modalità CBC possono essere disabilitati e possono essere utilizzati solo cifrari RC4 che non sono soggetti al difetto.

Inoltre, se SSLv2 è abilitato, ciò può causare un falso positivo per questa vulnerabilità. È molto importante disabilitare SSL v2.

Soluzione

> **Attenzione**: Se si utilizza un codice precedente di AsyncOS for Email Security, si consiglia di eseguire l'aggiornamento alla versione 11.0.3 o successive. Consulta le Note di rilascio di Cisco Email Security per informazioni e versioni più recenti. Per ulteriore assistenza nell'aggiornamento o nella disabilitazione delle cifrature, aprire una richiesta di assistenza.

Disabilitare i cifrari in modalità CBC per lasciare abilitati solo i cifrari RC4. Impostare il dispositivo in modo che utilizzi solo TLS v1 o TLS v1/TLS v1.2:

1. Accedere alla CLI.
2. Immettere il comando **sslconfig**.
3. Immettere il comando **GUI**.
4. Scegliere l'opzione numero 3 per "TLS v1" o come elencato in AsyncOS 9.6 "TLS v1/TLS v1.2".
5. Immettere la cifratura:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
6. Immettere il comando: **IN ENTRATA**.
7. Scegliere l'opzione numero 3 per "TLS v1" o come elencato in AsyncOS 9.6 "TLS v1/TLS v1.2".
8. Immettere la cifratura:
   `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`
9. Immettere il comando **OUTBOUND**.
10. Scegliere l'opzione numero 3 per "TLS v1" o come elencato in AsyncOS 9.6 "TLS v1/TLS v1.2".
11. Immettere la cifratura:
    `MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH:-EDH-RSA-DES-CBC3-SHA:-EDH-DSS-DES-CBC3-SHA:-DES-CBC3-SHA`

12. Premere **Invio** finché non si torna al prompt del nome host.
13. Immettere il comando **commit**.
14. Completare il commit delle modifiche.

L'ESA è ora configurata per supportare solo TLS v1, o TLSv1/TLS v1.2, con cifratura RC4 mentre non consente alcun filtro CBC.

Di seguito è riportato l'elenco dei cifrari utilizzati quando si imposta RC4:-SSLv2. Si noti che nell'elenco non sono presenti cifrari in modalità CBC.

```
ECDHE-RSA-RC4-SHA SSLv3 Kx=ECDH Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA SSLv3 Kx=ECDH Au=ECDSA Enc=RC4(128) Mac=SHA1
ADH-RC4-MD5 SSLv3 Kx=DH Au=None Enc=RC4(128) Mac=MD5
RC4-SHA SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
RC4-MD5 SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA SSLv3 Kx=PSK Au=PSK Enc=RC4(128) Mac=SHA1
EXP-ADH-RC4-MD5 SSLv3 Kx=DH(512) Au=None Enc=RC4(40) Mac=MD5 export
EXP-RC4-MD5 SSLv3 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
```

Anche se questo tipo di sfruttamento è di scarsissima preoccupazione a causa della sua complessità e dei requisiti da sfruttare, le prestazioni di queste fasi sono una grande garanzia per la prevenzione di possibili attacchi, oltre che per superare rigorose scansioni di sicurezza.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems