Disattivazione delle crittografie in modalità CBC del server SSH su un'ASA

Sommario

Introduzione

In questo documento viene descritto come disabilitare la modalità CBC del server SSH sulle appliance ASA. Sulla vulnerabilità della scansione CVE-2008-5161 è documentato che l'uso di un algoritmo di cifratura a blocchi in modalità CBC (Cipher Block Chaining), rende più facile per gli attaccanti remoti recuperare alcuni dati di testo normale da un blocco arbitrario di testo cifrato in una sessione SSH tramite vettori sconosciuti.

CBC (Cipher Block Chaining) è una modalità operativa per i blocchi cifrati. Questo algoritmo utilizza una cifratura a blocchi per fornire un servizio informativo, ad esempio la riservatezza o l'autenticità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Architettura della piattaforma ASA Adaptive Security Appliance
- CBC (Cipher Block Chaining)

Componenti usati

Per questo documento, è stato usato uno switch Cisco ASA 5506 con sistema operativo 9.6.1.

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.

Problema

Per impostazione predefinita, sull'appliance ASA la modalità CBC è abilitata, il che potrebbe rappresentare una vulnerabilità per le informazioni dei clienti.

Soluzione

Dopo il miglioramento di CSCum63371, la possibilità di modificare i cifrari SSH ASA è stata introdotta nella versione 9.1(7), ma la versione che dispone ufficialmente dei comandi ssh cipher encryption e ssh cipher integration è la 9.6.1.

Per disabilitare la funzione CBC Mode Ciphers sul protocollo SSH, attenersi alla seguente procedura:

Eseguire "sh run all ssh" sull'appliance ASA:

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption medium
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

Se si visualizza il comando ssh cipher encryption medium, l'ASA utilizza cifrari di media ed elevata potenza, impostazione predefinita sull'appliance ASA.

Per visualizzare gli algoritmi di crittografia ssh disponibili nell'appliance ASA, eseguire il comando show ssh ciphers:

```
ASA(config)# show ssh ciphers
Available SSH Encryption and Integrity Algorithms Encryption Algorithms:
        all:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        low:     3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        medium:  3des-cbc     aes128-cbc   aes192-cbc   aes256-cbc   aes128-ctr   aes192-ctr   aes256-c
        fips:    aes128-cbc   aes256-cbc
        high:    aes256-cbc   aes256-ctr
Integrity Algorithms:
        all:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
        low:     hmac-sha1    hmac-sha1-96 hmac-md5     hmac-md5-96
        medium:  hmac-sha1    hmac-sha1-96
        fips:    hmac-sha1
        high:    hmac-sha1
```

L'output mostra tutti gli algoritmi di crittografia disponibili: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr.

Per disabilitare la modalità CBC in modo che possa essere utilizzata sulla configurazione ssh,

personalizzare gli algoritmi di crittografia da utilizzare con il comando seguente:

```
ssh cipher encryption custom aes128-ctr:aes192-ctr:aes256-ctr
```

Al termine, eseguire il comando show run all ssh. Nella configurazione della crittografia ssh, tutti gli algoritmi usano solo la modalità CTR:

```
ASA(config)# show run all ssh
ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 outside
ssh timeout 60
ssh version 2
ssh cipher encryption custom "aes128-ctr:aes192-ctr:aes256-ctr"
ssh cipher integrity medium
ssh key-exchange group dh-group1-sha1
```

Analogamente, gli algoritmi di integrità SSH possono essere modificati con il comando ssh cipher integration.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).