Wie stelle ich sicher, dass meine ESA nur SSH-Verbindungen von Clients akzeptiert, die SSH v2 verwenden?

Inhalt

Einführung

Dieses Dokument beschreibt, wie SSH-Authentifizierungsversionen auf der Cisco E-Mail Security Appliance (ESA) überprüft und konfiguriert werden.

Wie stelle ich sicher, dass meine ESA nur SSH-Verbindungen von Clients akzeptiert, die SSH v2 verwenden?

Die ESA kann so konfiguriert werden, dass Secure Shell (SSH)-Verbindungen zulässig sind. SSH-Verbindungen verschlüsseln den Datenverkehr zwischen dem angeschlossenen Host und der ESA. Dies schützt Authentifizierungsinformationen wie Benutzername und Kennwörter. Es gibt zwei Hauptversionen des SSH-Protokolls: Version 1 (SSH v1) und Version 2 (SSH v2). Da SSH v2 jünger ist, ist es sicherer als SSH v1. Daher ziehen es viele ESA-Administratoren vor, nur Verbindungen von Clients zuzulassen, die SSH v2 verwenden.

In Versionen von AsyncOS bis 7.6.3 können SSH v1-Verbindungen über die CLI mit **sshconfig** deaktiviert werden:

```
mail3.example.com> sshconfig
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings.
[]> setup
SSH v1 is currently ENABLED.
Choose the operation you want to perform:
- DISABLE - Disable SSH v1
[]> DISABLE
```

Bei Versionen von AsyncOS 8.x und neueren Versionen ist die Option zur Deaktivierung von SSH v1 mit **sshconfig** nicht verfügbar. Wenn SSH v1 vor dem Upgrade von 8.x aktiviert wurde, bleibt

SSH v1 aktiviert und auf der ESA verfügbar, auch nachdem das Upgrade abgeschlossen ist, obwohl alle Unterstützung für SSH v1 entfernt wurde. Dies kann ein Problem für Administratoren sein, die regelmäßige Sicherheitsprüfungen und Penetrationstests durchführen.

Da alle Unterstützung für SSH v1 entfernt wurde, muss eine Support-Anfrage geöffnet werden, damit SSHv1 deaktiviert ist.

Führen Sie den folgenden Befehl von einem externen Linux/Unix-Host oder einer anderen geeigneten CLI-Verbindung der Wahl aus, um zu überprüfen, ob SSH v1 für die betreffende ESA aktiviert oder deaktiviert ist:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Protocol major versions differ: 1 vs. 2
```

Die erwartete Ausgabe lautet "Hauptversionen des Protokolls unterscheiden sich: 1 vs. 2", was signalisieren würde, dass SSH v1 deaktiviert ist. Ist dies nicht der Fall, wird SSH v1 weiterhin aktiviert.

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Password:
Response:
Last login: Thu Oct 30 14:53:40 2014 from 192.168.0.3
Copyright (c) 2001-2013, Cisco Systems, Inc.

AsyncOS 8.0.1 for Cisco IronPort C360 build 023

Welcome to the Cisco IronPort C360 Messaging Gateway(tm) Appliance
myesa.local>
```

Diese Ausgabe würde signalisieren, dass SSH v1 noch verwendet wird und nach einem Upgrade auf 8.x oder höher zu Unsicherheit bei der ESA führen kann. Dies kann bei einem Penetrationstest oder einer Sicherheitsprüfung zur Kenntnis gebracht werden und eine erhebliche Lücke erkennen. Um dies zu korrigieren, müssen Sie ein Support-Ticket öffnen und eine entsprechende Korrektur anfordern. Sie müssen in der Lage sein, einen Support-Tunnel von der ESA für den technischen Support von Cisco bereitzustellen.

Zugehörige Informationen

- CSCuo46017: SSHv1 bleibt nach dem Upgrade aktiviert und kann nicht deaktiviert werden.
- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems