Fehlerbehebung bei SSH-Authentifizierungsfehlern auf ASA mit RADIUS unter Verwendung eines einmaligen Kennworts

Inhalt

Problem

Der SSH-Zugriff (Secure Shell) auf die ASA-Software (Adaptive Security Appliance) mit RADIUS (Remote Authentication Dial-In User Service) über OTP (One Time Password) schlägt fehl, wenn Cisco SSH Stack aktiviert ist.

Diese Syslog-Meldungen werden generiert:

```
Nov 14 2025 16:28:35: %ASA-6-113010: AAA challenge received for user from server .
Nov 14 2025 16:28:35: %ASA-4-109033: Authentication failed for admin user from . Interactive challenge
```

Umwelt

Die Symptome werden beobachtet, wenn alle Bedingungen übereinstimmen:

- Sichere Firewall 1230 mit ASA im Einzel- oder Multi-Kontext-Modus Auch andere Hardwareplattformen sind betroffen.
- Der RADIUS-Server wird für die SSH-Authentifizierung verwendet:

<#root>

```
device#
```

show run | i aaa

```
aaa-server RAD-OTP protocol radius
aaa-server RAD-OTP (management) host 192.0.2.1
aaa-server RAD-OTP (management) host 192.0.2.2
aaa authentication ssh console RAD-OTP
```

- Der RADIUS-Server fordert einen gültigen OTP-Code oder eine gültige Aufforderung zur erfolgreichen Authentifizierung an und erfordert diese.
- Cisco SSH-Stack ist auf ASA aktiviert.
- In Version 9.19.1 und höher ist der CiscoSSH-Stack standardmäßig aktiviert und kann optional mit dem Befehl no ssh stack cisco deaktiviert werden. Verwenden Sie den Befehl show ssh zur Überprüfung:

<#root>

```
device#

show ssh


ssh secure copy : ENABLED

ciscoSSH stack : DISABLED
```

- In Version 9.23.1 und höher kann dieser Stack nicht deaktiviert oder überprüft werden.

Auflösung

Die Symptome wurden im internen Labor erfolgreich reproduziert und unter der Cisco Bug-ID CSCwt57790 verfolgt.

Verwenden Sie eine der folgenden Problemumgehungsoptionen in den betroffenen Versionen:

- Lokale Authentifizierung für SSH-Verbindungen verwenden.
- Deaktivieren Sie auf dem RADIUS-Server die OTP-Anforderung für ASA.
- Deaktivieren Sie in vor Version 9.23 den CiscoSSH-Stack mit dem Befehl no ssh stack cisco. Überprüfen Sie die Cisco Secure Firewall ASA Series Command Reference, S

Commands, und bewerten Sie die möglichen Auswirkungen einer Deaktivierung des Cisco SSH-Stacks.

Ursache

Die Ursache für den Authentifizierungsfehler ist die Cisco Bug-ID CSCwt57790.

Verwandte Inhalte

- Cisco Bug-ID CSCwi04513
- Cisco Bug-ID CSCwt57790
- Befehlsreferenz für die Cisco Secure Firewall der ASA-Serie, S Befehle

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.