

Anmeldung an der ISE-Admin-GUI schlägt mit PingID-Federation-RADIUS-Token fehl

Inhalt

Problem

Die Anmeldung der Administrator-GUI bei der Cisco ISE schlägt fehl, wenn der PingID-Verbund als RADIUS-Token verwendet wird, obwohl die Paketerfassung zeigt, dass Ping Federate eine Access-Accept-Antwort zurückgibt. Der Anmeldefehler tritt auf, obwohl die RADIUS-Authentifizierung aus Netzwerksicht erfolgreich zu sein scheint, wodurch der administrative Zugriff auf die ISE-Schnittstelle verhindert wird. Die Netzwerkpaketanalyse bestätigt, dass der PingID-Server (10.32.154.200) die erwartete Access-Accept-Antwort an die ISE (10.2.200.241) sendet, der ISE-Admin-Anmeldevorgang jedoch weiterhin nicht erfolgreich abgeschlossen werden kann.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.3 Patch 7
- VM-Bereitstellung mit 4 Knoten
- PingID-Federation konfiguriert als RADIUS-Tokenauthentifizierung
- ISE-IP-Adresse: 10.2.200.241
- PingID-Server-IP-Adresse: 10.32.154.200
- Die Konfiguration des Administratorzugriffs wurde unter Administration > Admin Access überprüft.

Auflösung

Das Problem wurde durch eine Problemumgehung behoben, die eine erfolgreiche Admin-

Anmeldefunktion ermöglichte. Die in den folgenden Abschnitten beschriebenen Schritte wurden zur Behebung des Problems durchgeführt.

Schritt 1: Sammlung und Analyse von Beweismitteln

Der Paketerfassungsnachweis wurde erfasst und analysiert, um den RADIUS-Authentifizierungsfluss zwischen der ISE und dem PingID-Server zu bestätigen. Die Analyse hat bestätigt, dass Ping Federate die richtigen Access-Accept-Antworten gesendet hat.

Phase 2: Belege von prrt-server.log

###

prrt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

Schritt 3: Was ist der Message-Authenticator?

Der Message-Authenticator ist ein Sicherheitsattribut, das in RADIUS-Paketen verwendet wird, um die Integrität und Authentizität der Nachrichten sicherzustellen, die zwischen Netzwerkgeräten und dem RADIUS-Server ausgetauscht werden. Es handelt sich um eine kryptografische Signatur, die mithilfe von HMAC-MD5 über das gesamte RADIUS-Paket mit einem gemeinsamen geheimen Schlüssel berechnet wird. Dieses Attribut schützt vor Manipulationen und Spoofing von RADIUS-Nachrichten, insbesondere solche, die EAP-Authentifizierungsflüsse (Extensible Authentication Protocol) beinhalten.

Schritt 4: Workaround-Implementierung

Deaktivieren Sie "Message Authenticator Required On Response":

Verwaltung/Identitätsmanagement/Externe Identitätsquellen/RADIUS-Token. Klicken Sie auf den Namen des RADIUS-Tokens, und wechseln Sie dann zu Authentication (Authentifizierung).

Deaktivieren Sie die Option "Message Authenticator Required On Response".

Schritt 5: Validierungstests

Nach Anwendung der Problemumgehung wurden Admin-Anmeldetests ausgeführt, um die Lösung zu validieren. Diese Tests bestätigten die erfolgreiche Authentifizierung und den erfolgreichen Zugriff auf die ISE-Admin-GUI mithilfe des PingID-Verbunds als RADIUS-Token.

Schritt 6: Überwachungszeitraum

Es wurde ein Überwachungs- und Validierungszeitraum festgelegt, um die Stabilität des Workaround sicherzustellen. Während dieses Zeitraums wurden die Admin-Anmeldetests ohne gemeldete Fehler oder Fehler fortgesetzt.

Ursache

Der Fehler bei der ISE-Anmeldung für die Admin-GUI wurde durch eine Diskrepanz bei der RADIUS-Protokollsicherheitsdurchsetzung zwischen Cisco ISE 3.3 Patch 7 und PingID (Ping Federate) während der MFA-Authentifizierung verursacht.

Konkret:

- Für die Cisco ISE musste das RADIUS Message-Authenticator-Attribut in der Access-Accept-Antwort des externen RADIUS-Tokenservers vorhanden sein.
- PingID gab Access-Accept-Antworten ohne das Message-Authenticator-Attribut zurück.
- Da bei der ISE die Einstellung Message Authenticator Required On Response (Nachrichtenauthentifizierung bei Antwort erforderlich) aktiviert war, wurde die RADIUS-

Antwort ohne weitere Änderungen als ungültig zurückgewiesen, obwohl die Authentifizierung selbst auf der PingID-Seite erfolgreich war.

- Diese Durchsetzung ist Teil der Sicherheitsmaßnahmen der Cisco ISE zur Minimierung der Schwachstelle durch Blast-RADIUS (CVE-2024-3596).

Verwandte Inhalte

- [Eindämmung des Blast-RADIUS-Protokoll-Spoofing \(CVE-2024-3596\)](#)

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.