

El inicio de sesión GUI de ISE Admin falla con el token RADIUS de federación PingID

Contenido

Problema

El inicio de sesión GUI del administrador en Cisco ISE falla cuando se utiliza la federación de PingID como token RADIUS, a pesar de que las capturas de paquetes muestran que Ping Federate devuelve una respuesta de aceptación de acceso. El error de inicio de sesión se produce aunque la autenticación RADIUS parezca correcta desde una perspectiva de red, lo que impide el acceso administrativo a la interfaz ISE. El análisis de paquetes de red confirma que el servidor PingID (10.32.154.200) envía la respuesta de aceptación de acceso esperada a ISE (10.2.200.241), pero el proceso de inicio de sesión de administrador de ISE sigue sin completarse correctamente.

Entorno

- Parche 7 de Cisco Identity Services Engine (ISE) versión 3.3
- Implementación de VM de 4 nodos
- Federación de PingID configurada como autenticación de token RADIUS
- Dirección IP de ISE: 10.2.200.241
- Dirección IP del servidor PingID: 10.32.154.200
- Configuración de acceso de administrador revisada en Administración > Acceso de administrador

Resolución

El problema se resolvió mediante la aplicación de una solución alternativa que habilitó la funcionalidad de inicio de sesión de administrador exitoso. Se adoptaron las medidas descritas en las secciones siguientes para abordar el problema.

Paso 1: Recopilación y análisis de pruebas

Se recopilaron y analizaron pruebas de captura de paquetes para confirmar el flujo de autenticación RADIUS entre ISE y el servidor PingID. El análisis verificó que Ping Federate estaba enviando correctamente respuestas de aceptación de acceso.

Paso 2: Evidencia de port-server.log

###

prtr-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
```

###

Paso 3: ¿Qué es el autenticador de mensaje?

Message-Authenticator es un atributo de seguridad utilizado en paquetes RADIUS para garantizar la integridad y autenticidad de los mensajes intercambiados entre los dispositivos de red y el servidor RADIUS. Se trata de una firma criptográfica calculada mediante HMAC-MD5 en todo el paquete RADIUS con una clave secreta compartida. Este atributo ayuda a proteger contra la manipulación y la suplantación de los mensajes RADIUS, especialmente aquellos que implican flujos de autenticación de protocolo de autenticación extensible (EAP).

Paso 4: Implementación de solución alternativa

Deshabilitar "Se requiere autenticador de mensaje al responder": Administración/Gestión de identidades/Orígenes de identidad externos/Token RADIUS. Haga clic en el nombre del token RADIUS y, a continuación, vaya a Autenticación. Desmarque "Se requiere autenticador de mensaje al responder".

Paso 5: Pruebas de validación

Después de aplicar la solución alternativa, se ejecutaron pruebas de inicio de sesión de administrador para validar la resolución. Estas pruebas confirmaron una autenticación y un acceso correctos a la GUI de administración de ISE mediante la federación de PingID como el token RADIUS.

Paso 6: Período de supervisión

Se estableció un período de supervisión y validación para garantizar la estabilidad de la solución alternativa. Durante este período, se llevaron a cabo pruebas continuas de inicio de sesión de administrador sin que se notificaran errores o errores.

Causa

El error de inicio de sesión en la GUI de administración de ISE se debe a una discordancia de aplicación de seguridad del protocolo RADIUS entre Cisco ISE 3.3 Patch 7 y PingID (Ping Federate) durante la autenticación MFA.

Específicamente:

- Cisco ISE requería que el atributo `Message-Authenticator` de RADIUS estuviera presente en la respuesta `Access-Accept` del servidor de token RADIUS externo.
- PingID estaba devolviendo respuestas `Access-Accept` sin el atributo `Message-Authenticator`.
- Debido a que ISE tenía la configuración `Message Authenticator Required On Response`

habilitada, rechazó silenciosamente la respuesta RADIUS como no válida, aunque la autenticación en sí tuvo éxito en el lado PingID.

- Esta aplicación forma parte de la consolidación de la seguridad de Cisco ISE para mitigar la vulnerabilidad de Blast-RADIUS (CVE-2024-3596).

Contenido relacionado

- [Mitigación de la suplantación del protocolo Blast-RADIUS \(CVE-2024-3596\)](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).