Recomendaciones contra ataques mediante pulverización de contraseñas que afectan a los servicios VPN de acceso remoto

Contenido

Introducción

Este documento describe las recomendaciones que se deben considerar para evitar los fallos de asignación de token de host en Secure Firewall, derivados de ataques de pulverización de contraseña.

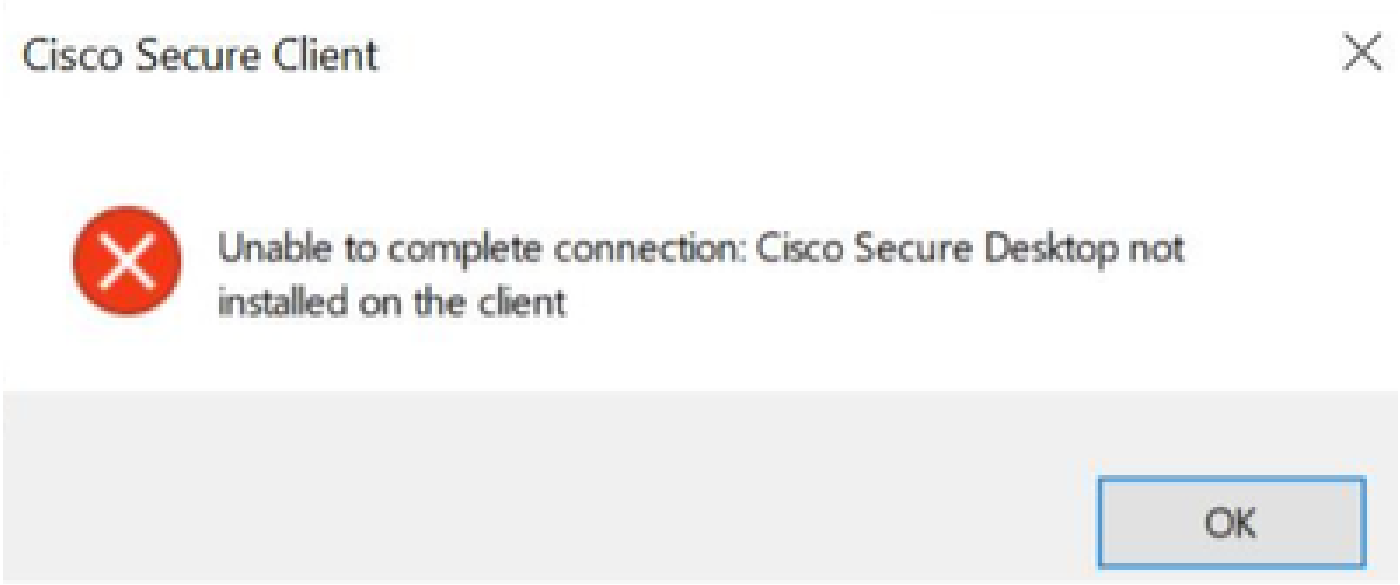
Antecedentes

Al intentar establecer una conexión RAVPN mediante Cisco Secure Client (AnyConnect), los usuarios pueden encontrar de forma intermitente un mensaje de error que indica "No se puede completar la conexión. Cisco Secure Desktop no está instalado en el cliente.". Este comportamiento suele producirse cuando se produce un error al asignar un token de análisis de host por parte de la cabecera de VPN, ya sea un dispositivo de seguridad adaptable (ASA) de firewall seguro de Cisco o una defensa frente a amenazas (FTD). En particular, esta falla de asignación se correlaciona con casos de ataques de fuerza bruta dirigidos a la infraestructura de Secure Firewall y actualmente se está tratando con la máxima urgencia bajo el ID de bug de Cisco CSCwj45822.

Comportamientos observados

No se pueden establecer conexiones VPN con Cisco Secure Client (AnyConnect) cuando la condición de firewall (HostScan) está habilitada

Al intentar establecer una conexión VPN mediante Cisco Secure Client (AnyConnect), los usuarios pueden encontrar de forma intermitente un mensaje de error que indica "No se puede completar la conexión. Cisco Secure Desktop no está instalado en el cliente". Este problema impide la finalización correcta del proceso de conexión VPN.



Nota: este comportamiento específico se produce únicamente cuando la condición del firewall (HostScan) está activada en la cabecera, independientemente de la versión de Secure Client o AnyConnect utilizada.

Agotamiento del token de Hostscan

La cabecera VPN Cisco Secure Firewall Adaptive Security Appliance (ASA) o Threat Defence (FTD) muestra síntomas de fallos de asignación de tokens de hostscan. Para verificar esto, ejecute el comando debug menu webvpn 187 0.

<#root>

```
ASA# debug menu webvpn 187 0
Allocated Hostscan token = 1000
```

Hostscan token allocate failure = xxx - - - - > Increments

Nota: la aparición de este problema es consecuencia de los ataques. El asunto se está tratando actualmente con la máxima urgencia bajo el ID de bug Cisco CSCwj45822.

Cantidad inusual de solicitudes de autenticación

El Cisco Secure Firewall ASA o FTD de cabecera de VPN muestra síntomas de ataques de pulverización de contraseñas con 100 000 o millones de intentos de autenticación rechazados.

Nota: Estos inusuales intentos de autenticación pueden dirigirse hacia la base de datos LOCAL o hacia servidores de autenticación externos.

La mejor manera de detectar esto es mirando el syslog. Busque un número inusual de cualquiera de los siguientes ID de syslog de ASA:

- %ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database :

user

= *admin* : user

IP

= *x.x.x.x*

- %ASA-6-113005

<#root>

%ASA-6-113005

```
: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =
```

- %ASA-6-716039

<#root>

%ASA-6-716039

```
: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.
```

El nombre de usuario siempre está oculto hasta que se configura el comando no logging hide username en el ASA.

Nota: Esto permite comprobar si las IP infractoras generan o conocen usuarios válidos; sin embargo, tenga cuidado, ya que los nombres de usuario serán visibles en los registros.

Para verificarlo, inicie sesión en la Interfaz de línea de comandos (CLI) de ASA o FTD, ejecute el comando show aaa-server e investigue el número inusual de solicitudes de autenticación intentadas y rechazadas a cualquiera de los servidores AAA configurados:

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against external server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms

Number of authentication requests 2228536 - - - - - >>>> Unusual increments


Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312

Number of rejects 2225363 - - - - - >>>> Unusual increments / Unusual rejection rate


Number of challenges 0
```

```
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
Number of unrecognized responses 0
```

Recomendaciones

Si bien actualmente no existe una solución única para eliminar por completo el riesgo, puede revisar y aplicar las siguientes prácticas recomendadas, que están diseñadas para ayudar a reducir la probabilidad de ocurrencia y disminuir el impacto de estos ataques de fuerza bruta en sus conexiones RAVPN.

1. Activar registro

El registro es una parte crucial de la ciberseguridad que implica registrar los eventos que se producen dentro de un sistema. La ausencia de registros detallados deja lagunas en la comprensión, lo que dificulta un análisis claro del método de ataque. Se recomienda habilitar el registro en un servidor syslog remoto para mejorar la correlación y la auditoría de los incidentes de seguridad y de red en varios dispositivos de red.

Para obtener información sobre cómo configurar el registro, consulte las siguientes guías específicas de la plataforma:

Software Cisco ASA:

- Guía de uso para proteger el firewall ASA
- Capítulo de registro de la Guía de configuración de CLI de operaciones generales de Cisco Secure Firewall ASA Series

Software Cisco FTD:

- Configuración del inicio de sesión en FTD mediante Firewall Management Center (FMC)
- Sección Configure Syslog en el capítulo Platform Settings de la Guía de configuración de dispositivos de Cisco Secure Firewall Management Center
- Configuración y verificación de Syslog en el administrador de dispositivos Firepower
- Configuración de la sección Configuración de registro del sistema del capítulo Configuración del sistema de la Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager

---

Nota: Los ID de mensajes de syslog necesarios para verificar los comportamientos descritos en este documento (113015, 113005 y 716039) deben estar habilitados en el nivel

---

informativo (6). Estos ID pertenecen a las clases de registro 'auth' y 'webvpn'.

2. Aplicar medidas de refuerzo para VPN de acceso remoto

Para mitigar el impacto de estos ataques, implemente las siguientes medidas de endurecimiento:

1. Inhabilitación de la Autenticación AAA en los Perfiles de Conexión DefaultWEBVPN y DefaultRAGroup (paso a paso: ASA | FTD gestionado por FMC).
2. Desactivar la condición de firewall seguro (Hostscan) de DefaultWEBVPNGroup y DefaultRAGroup (paso a paso: ASA | FTD gestionado por FMC).
3. Desactivar los alias de grupo y activar las URL de grupo en el resto de los perfiles de conexión (paso a paso: ASA) | FTD gestionado por FMC).

Nota: si necesita asistencia con FTD gestionado a través de la gestión de dispositivos de firewall (FDM) local, póngase en contacto con el centro de asistencia técnica (TAC) para obtener asesoramiento de expertos.

Para obtener más información, consulte la guía Implementación de medidas de refuerzo para AnyConnect VPN de Secure Client.

3. Bloquear intentos de conexión de orígenes malintencionados

Para impedir los intentos de conexión de fuentes no autorizadas, puede implementar cualquiera de las opciones que se enumeran a continuación:

Implementación de ACL a nivel de interfaz

Implemente una ACL de nivel de interfaz en el ASA/FTD para filtrar las direcciones IP públicas no autorizadas y evitar que inicien sesiones VPN remotas.

Utilice el comando "shun"

Se trata de un enfoque sencillo para bloquear una IP malintencionada; sin embargo, debe hacerse de forma manual. Lea la sección Configuración alternativa para bloquear los ataques de firewall seguro mediante el comando 'shun' para obtener más información.

Configurar ACL del plano de control

Implemente una ACL de plano de control en el ASA/FTD para filtrar las direcciones IP públicas no autorizadas y evitar que inicien sesiones VPN remotas. Configure las políticas de control de acceso del plano de control para Secure Firewall Threat Defence y ASA.

Nota: Cisco Talos ha publicado una lista de direcciones IP y credenciales asociadas a estos ataques. Un enlace a su repositorio de GitHub se puede encontrar en la sección "IOCs" de su aviso. Es importante tener en cuenta que las direcciones IP de origen para este tráfico probablemente cambien, por lo tanto, debe revisar los registros de seguridad (syslog) para identificar las direcciones IP problemáticas. Tras la identificación, cualquiera de las 3 opciones se puede utilizar para bloquearlas.

Implementaciones de endurecimiento adicionales para RAVPN

Las recomendaciones proporcionadas hasta el momento tienen como objetivo reducir el riesgo y el impacto de los ataques en los servicios RAVPN. Sin embargo, puede considerar contramedidas adicionales que requieran cambios adicionales en sus implementaciones para fortalecer la seguridad de su implementación de VPN de acceso remoto, como la adopción de la autenticación basada en certificados para RAVPN. Consulte el documento Implementación de Medidas de Refuerzo para Secure Client AnyConnect VPN para obtener una guía de configuración detallada.

Additional Information

- Procedimientos de investigación forense de Cisco ASA para los primeros en responder
- Procedimientos de investigación forense de Cisco Firepower Threat Defence para los primeros en responder
- Asesoramiento sobre amenazas de Cisco Talos
- Para obtener asistencia adicional, póngase en contacto con el Technical Assistance Center (TAC). Se necesita un contrato de asistencia válido: Contactos de asistencia globales de Cisco.

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).