Mitigación de la suplantación de protocolo Blast-RADIUS (CVE-2024-3596)

Contenido

Introducción

El 7 de julio de 2024, los investigadores de seguridad revelaron la siguiente vulnerabilidad en el protocolo RADIUS: CVE-2024-3596: El protocolo RADIUS en RFC 2865 es susceptible a ataques de falsificación por parte de un atacante en ruta que puede modificar cualquier respuesta válida (Access-Accept, Access-Reject o Access-Challenge) a cualquier otra respuesta mediante un ataque de colisión de prefijo seleccionado contra la firma MD5 Response Authenticator. Han publicado un documento que detalla sus hallazgos en https://www.blastradius.fail/pdf/radius.pdf que demuestra una falsificación de respuesta exitosa contra flujos que no utilizan el atributo Message-Authenticator.

Para obtener una lista actualizada de los productos de Cisco afectados por esta vulnerabilidad y de las versiones que contienen correcciones, visite: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. En este artículo se tratan las técnicas generales de mitigación, así como la forma en que se aplican a algunos productos de Cisco, pero no a todos ellos. Se debe consultar la documentación de cada producto para obtener información específica. Como servidor RADIUS emblemático de Cisco, Identity Service Engine se tratará con más detalle.

Background

Este ataque aprovecha un ataque de prefijo seleccionado MD5 que utiliza colisiones en MD5, lo que permite que un atacante agregue datos adicionales al paquete de respuesta RADIUS mientras modifica los atributos existentes del paquete de respuesta. Un ejemplo que se demostró fue la capacidad de cambiar un rechazo de acceso RADIUS a un aceptación de acceso RADIUS. Esto es posible porque RADIUS de forma predeterminada no incluye un hash de todos los atributos en el paquete. RFC 2869 agrega el atributo Message-Authenticator, pero actualmente solo es necesario incluirlo cuando se utilizan protocolos EAP, lo que significa que el ataque descrito en CVE-2024-3596 es posible contra cualquier intercambio no EAP en el que el cliente RADIUS (NAD) no incluya el atributo Message-Authenticator.

Mitigación

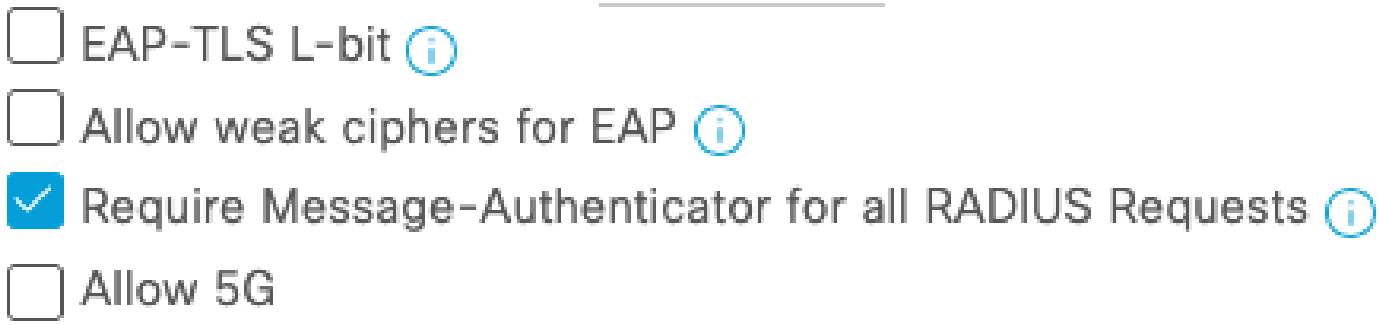
Autenticador de mensaje

1) El cliente RADIUS debe incluir el atributo Message-Authenticator.

Cuando el dispositivo de acceso a la red (NAD) incluye el atributo Message-Authenticator en la solicitud de acceso, Identity Services Engine incluirá Message-Authenticator en el paquete Access-Accept, Access-Challenge o Access-Reject resultante en todas las versiones.

2) El servidor RADIUS debe forzar la recepción del atributo Message-Authenticator.

No basta con incluir el autenticador de mensaje en la solicitud de acceso, ya que el ataque permite eliminar el autenticador de mensaje de la solicitud de acceso antes de reenviarlo al servidor RADIUS. El servidor RADIUS también debe requerir que NAD incluya el autenticador de mensaje en la solicitud de acceso. Esto no es lo predeterminado en Identity Services Engine, pero se puede habilitar en el nivel de protocolos permitidos, que se aplica en el nivel de conjunto de políticas. La opción bajo la configuración de Protocolos permitidos es "Requerir autenticador de mensaje" para todas las solicitudes RADIUS":



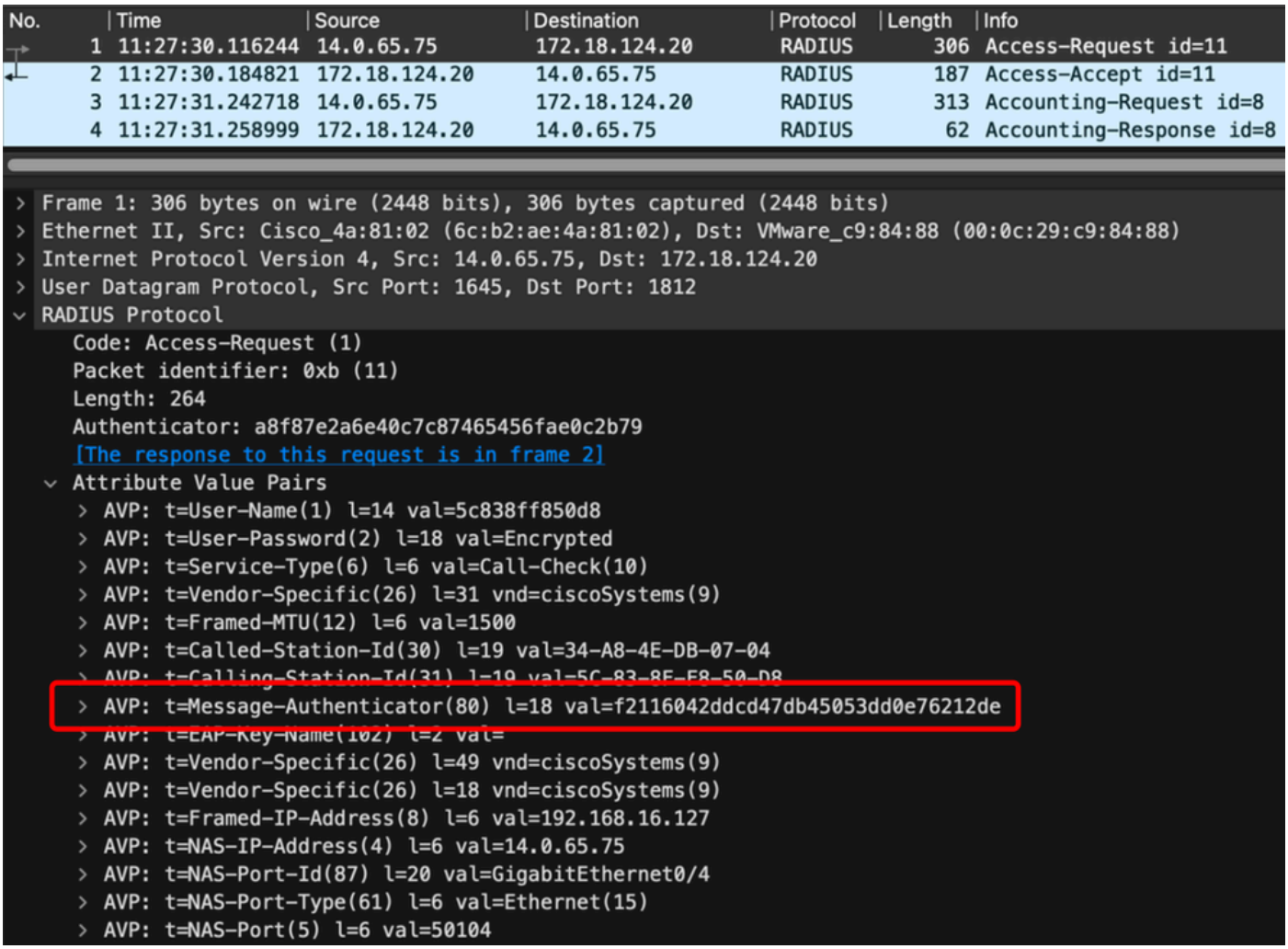
Opción de protocolos permitidos en Identity Services Engine

Las autenticaciones que coinciden con un conjunto de políticas donde la configuración de protocolos permitidos requiere Message-Authenticator, pero donde Access-Request no contiene el atributo Message-Authenticator serán descartadas por ISE:

Event	5405 RADIUS Request dropped
Failure Reason	11057 Message-Authenticator attribute is missing in RADIUS Access-Request

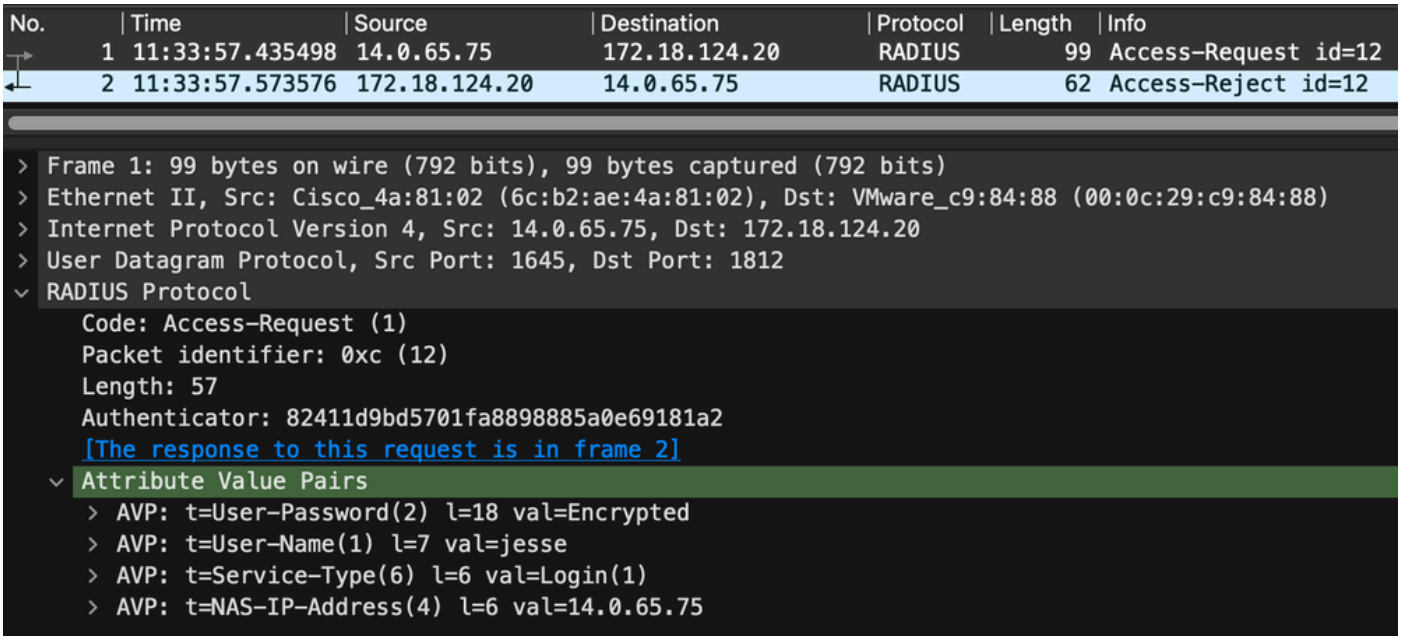
Es importante verificar si el NAD está enviando Message-Authenticator antes de ser requerido por el servidor RADIUS ya que este no es un atributo negociado, depende del NAD enviarlo de forma predeterminada o configurarlo para enviarlo. Message-Authenticator no es uno de los atributos notificados por ISE; una captura de paquetes es la mejor manera de determinar si un NAD/caso de uso incluye Message-Authenticator. ISE ha incorporado la funcionalidad de captura de paquetes en Operaciones -> Solucionar problemas -> Herramientas de diagnóstico -> Herramientas generales -> Volcado de TCP. Tenga en cuenta que diferentes casos de uso del mismo NAD pueden incluir o no Message-Authenticator.

A continuación se muestra un ejemplo de captura de una solicitud de acceso que incluye el atributo Message-Authenticator:



Atributo de autenticador de mensaje en la solicitud de acceso a Radius

A continuación se muestra un ejemplo de captura de una solicitud de acceso que no incluye el atributo Message-Authenticator:



Cifrar con TLS/IPSec

La solución más eficaz a largo plazo para proteger RADIUS es cifrar el tráfico entre el servidor RADIUS y el NAD. Esto añade privacidad y una mayor integridad criptográfica a la mera confianza en el autenticador de mensaje derivado de MD5-HMAC. El cual, si cualquiera de estos puede ser utilizado entre el servidor RADIUS y el NAD, depende de ambos lados que soportan el método de encripción.

Los términos generales utilizados en el sector para el cifrado TLS de RADIUS son:

- "RadSec": hace referencia a RFC 6614
- "RadSec TLS": hace referencia a RFC 6614
- "RadSec DTLS": hace referencia a RFC 7360

Es importante implementar el cifrado de forma controlada, ya que el cifrado TLS presenta una sobrecarga de rendimiento, así como consideraciones de administración de certificados. Los certificados también tendrán que renovarse periódicamente.

RADIUS sobre DTLS

La seguridad de la capa de transporte del datagrama (DTLS) como una capa de transporte para RADIUS está definida por RFC 7360, que utiliza certificados para autenticar mutuamente el servidor RADIUS y el NAD luego cifra el paquete RADIUS completo mediante un túnel TLS. El método de transporte sigue siendo UDP y requiere que los certificados se implementen tanto en el servidor RADIUS como en NAD. Tenga en cuenta que al implementar RADIUS sobre DTLS, es imperativo que el vencimiento y la sustitución de certificados se administre de cerca para evitar que los certificados caducados interrumpan la comunicación RADIUS. ISE admite DTLS para la comunicación entre ISE y NAD, ya que no se admite RADIUS 3.4 Radius sobre DTLS para servidores proxy RADIUS o servidores de token RADIUS. RADIUS sobre DTLS también es compatible con muchos dispositivos de Cisco que actúan como NAD, como switches y controladores inalámbricos que ejecutan IOS-XE®.

RADIUS sobre TLS

El cifrado de seguridad de la capa de transporte (TLS) para RADIUS se define en RFC 6614, cambia el transporte a TCP y utiliza TLS para cifrar completamente los paquetes RADIUS. Esto es comúnmente utilizado por el servicio eduroam como ejemplo. A partir de ISE 3.4, RADIUS sobre TLS no es compatible, pero sí lo son muchos dispositivos de Cisco que actúan como NAD, como switches y controladores inalámbricos que ejecutan IOS-XE.

IPSec

Identity Services Engine admite de forma nativa túneles IPSec entre ISE y NAD que también admiten túneles IPSec de terminación. Se trata de una buena opción en la que no se admite RADIUS sobre DTLS o RADIUS sobre TLS, pero se debe utilizar con moderación, ya que solo se admiten 150 túneles por nodo de servicios de políticas de ISE. ISE 3.3 y las versiones posteriores ya no necesitan una licencia para IPSec; ahora está disponible de forma nativa.

Mitigación parcial

Segmentación RADIUS

Segmente el tráfico RADIUS en las VLAN de gestión y los enlaces seguros y cifrados, como los que se pueden proporcionar a través de SD-WAN o MACSec. Esta estrategia no reduce el riesgo de ataque a cero, pero puede reducir considerablemente la superficie de ataque de la vulnerabilidad. Esto puede ser una buena medida de interrupción de parada mientras los productos despliegan el requisito de autenticador de mensaje o soporte DTLS/RadSec. La vulnerabilidad requiere que un atacante realice correctamente la comunicación RADIUS Man-in-the-Middle (MITM), de modo que si un atacante no puede entrar en un segmento de red con ese tráfico, el ataque no es posible. La razón por la que esto es sólo una mitigación parcial es que una configuración incorrecta de la red o una vulnerabilidad de una parte de la red puede exponer el tráfico RADIUS.

Si el tráfico RADIUS no se puede segmentar o cifrar, se pueden implementar funciones adicionales para evitar MITM exitoso en segmentos en riesgo como: IP Source Guard, Dynamic ARP Inspection y DHCP Snooping. También puede ser posible utilizar otros métodos de autenticación basados en el tipo de flujo de autenticación como TACACS+, SAML, LDAPS, etc.

Estado de vulnerabilidad de Identity Services Engine

Las tablas siguientes describen lo que está disponible a partir de ISE 3.4 para proteger los flujos de autenticación frente a Blast-RADIUS. Para recapitular, los siguientes 3 elementos deben estar disponibles para un flujo que utilice únicamente el autenticador de mensaje y no el cifrado DTLS/RadSec/IPSec, para que el flujo no sea vulnerable:
1) El dispositivo de acceso a la red DEBE enviar el atributo Message-Authenticator en la solicitud de acceso.

2) El servidor RADIUS DEBE requerir el atributo Message-Authenticator en Access-Request.

3) El servidor RADIUS DEBE responder con el atributo Message-Authenticator en Access-Challenge, Access-Accept y Access-Reject.

Consulte CSCwk67747, que realiza un seguimiento de los cambios para cerrar las vulnerabilidades cuando ISE actúa como cliente RADIUS.

ISE como servidor RADIUS

AAA Scenario	ISE Config	NAD capabilities	Status	Alternative options
EAP Protocols	--	--	Protected	
MAB, PAP, CHAP, MSCHAPv1/v2, Authorize-Only	Have on the checkbox "Require Message-Authenticator for all protocols"	Supports Message-Authenticator for non-EAP protocols	Protected	
		Doesn't support Message-Authenticator for non-EAP protocols	Vulnerable (because of NAD)	Can use IPsec
	Use RADIUS DTLS for this NAD	Supports RADIUS DTLS	Protected	
		Doesn't support RADIUS DTLS	Vulnerable (because of NAD)	Can use IPsec

ISE como cliente RADIUS

AAA Scenario	ISE Config	Peers' capabilities	Status	Alternative options
ISE as RADIUS Proxy	--	NAD supports Message-Authenticator **AND** RADIUS Server supports Message-Authenticator	Protected	
		NAD doesn't support Message-Authenticator **OR** RADIUS Server doesn't support Message-Authenticator	Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if both NAD and RADIUS Server use Message-Authenticator
ISE as RADIUS Token Client	--		Vulnerable (ISE must send Message-Authenticator to RADIUS Server and must require it in response)	Can use IPsec Partial mitigation is achieved if RADIUS Token Server uses Message-Authenticator
ISE as CoA Client	Configured to use Message-		Vulnerable (ISE must require	Can use IPsec Partial mitigation is achieved if Device Profiler checked option to use Message-Authenticator

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).