Mitigação de Falsificação de Protocolo Blast-RADIUS (CVE-2024-3596)

Contents

Introdução

Em 7 de julho de 2024, os pesquisadores de segurança revelaram a seguinte vulnerabilidade no protocolo RADIUS: CVE-2024-3596: O protocolo RADIUS sob o RFC 2865 é susceptível a ataques falsificados por um invasor no caminho que pode modificar qualquer Resposta válida (Access-Accept, Access-Reject ou Access-Challenge) para qualquer outra resposta usando um ataque de colisão de prefixo escolhido contra a assinatura do Autenticador de Resposta MD5. Eles publicaram um documento detalhando suas descobertas em https://www.blastradius.fail/pdf/radius.pdf que demonstra uma falsificação de resposta bem-sucedida contra fluxos que não utilizam o atributo Autenticador de mensagem.

Para obter uma lista atualizada dos produtos Cisco afetados por essa vulnerabilidade e versões que contêm correções, visite: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. Este artigo abordará as técnicas gerais de mitigação e como elas se aplicam a alguns, mas não a todos, produtos da Cisco; a documentação individual dos produtos deve ser consultada para obter detalhes. Como o principal servidor RADIUS da Cisco, o Identity Service Engine será abordado com mais detalhes.

Background

Esse ataque aproveita um ataque de prefixo escolhido MD5 utilizando colisões em MD5, o que permite que um invasor adicione dados adicionais ao pacote de resposta RADIUS enquanto modifica atributos existentes do pacote de resposta. Um exemplo demonstrado foi a capacidade de alterar um RADIUS Access-Reject em um RADIUS Access-Accept. Isso é possível porque o RADIUS por padrão não inclui um hash de todos os atributos no pacote. O RFC 2869 adiciona o atributo Autenticador de mensagem, mas atualmente ele só precisa ser incluído ao usar protocolos EAP, o que significa que o ataque descrito no CVE-2024-3596 é possível contra qualquer intercâmbio não EAP onde o Cliente RADIUS (NAD) não inclui o atributo Autenticador de mensagem.

Atenuação

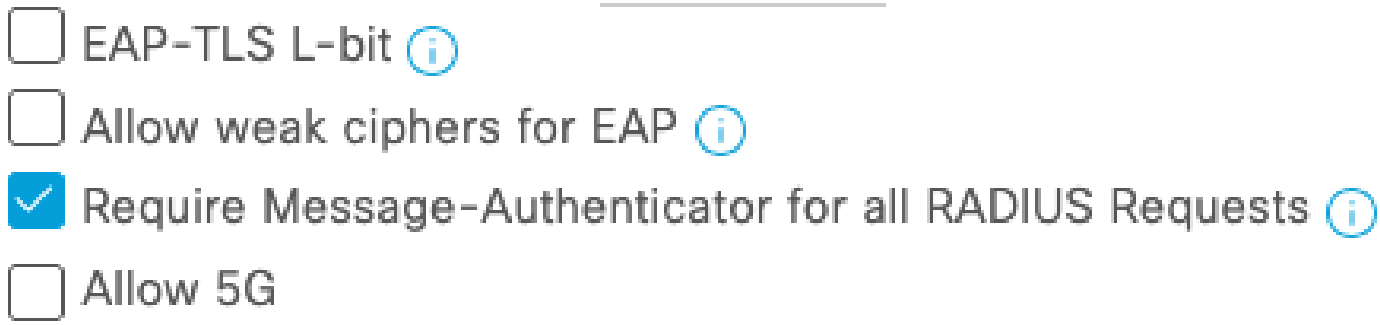
Autenticador de mensagem

1) O cliente RADIUS deve incluir o atributo Message-Authenticator.

Quando o Network Access Device (NAD) inclui o atributo Message-Authenticator na solicitação de acesso, o Identity Services Engine inclui o Message-Authenticator no pacote resultante Access-Accept, Access-Challenge ou Access-Reject em todas as versões.

2) O servidor RADIUS deve impor o recebimento do atributo Message-Authenticator.

Não basta incluir o Autenticador de Mensagem na Solicitação de Acesso, pois o ataque possibilita retirar o Autenticador de Mensagem da Solicitação de Acesso antes que ele seja encaminhado ao Servidor RADIUS. O servidor RADIUS também deve exigir que o NAD inclua Message-Authenticator na solicitação de acesso. Esse não é o padrão no Identity Services Engine, mas pode ser habilitado no nível de protocolos permitidos, que se aplica no nível do conjunto de políticas. A opção na configuração de protocolos permitidos é "Exigir autenticador de mensagem" para todas as solicitações RADIUS:



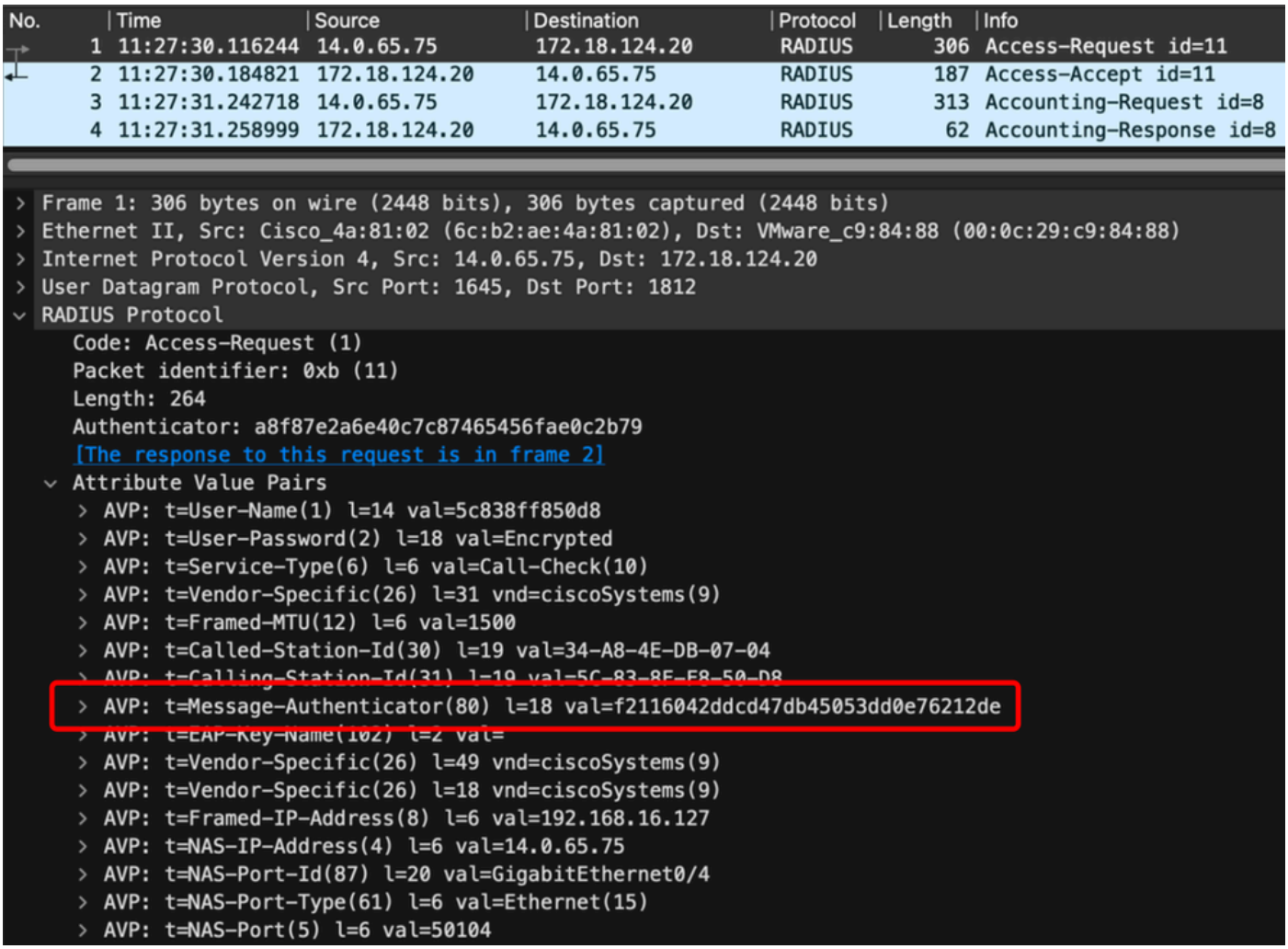
Opção de protocolos permitidos no Identity Services Engine

As autenticações que correspondem a um conjunto de políticas em que a configuração de protocolos permitidos requer o Message-Authenticator, mas em que a solicitação de acesso não contém o atributo Message-Authenticator, serão eliminadas pelo ISE:

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

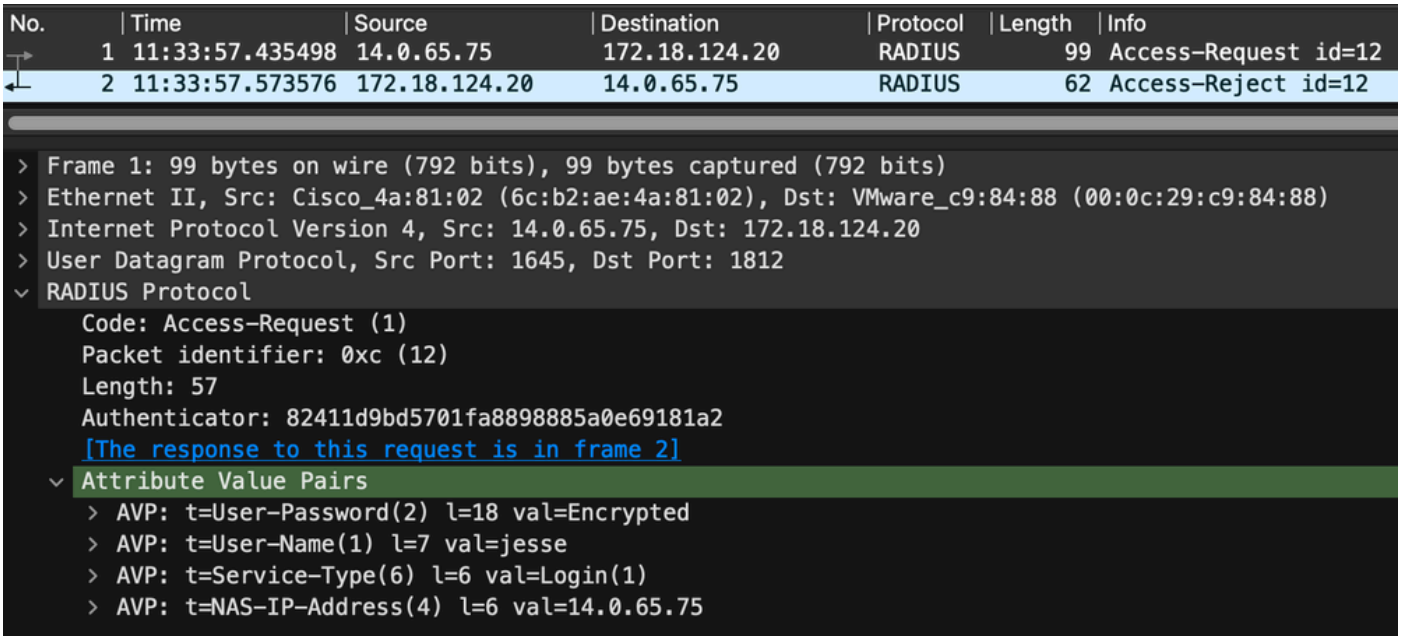
É importante verificar se o NAD está enviando Message-Authenticator antes de ser exigido pelo servidor RADIUS, pois esse não é um atributo negociado. Cabe ao NAD enviá-lo por padrão ou configurá-lo para enviá-lo. O Message-Authenticator não é um dos atributos relatados pelo ISE, uma captura de pacote é a melhor maneira de determinar se um NAD/caso de uso está incluindo o Message-Authenticator. O ISE incorporou a funcionalidade de captura de pacotes em Operations -> Troubleshoot -> Diagnostic Tools -> General Tools -> TCP Dump. Lembre-se de que casos de uso diferentes do mesmo NAD podem incluir ou não o Autenticador de mensagem.

Veja a seguir um exemplo de captura de uma solicitação de acesso que inclui o atributo Autenticador de mensagem:



Atributo Message-authenticator em solicitação de acesso Radius

Veja a seguir um exemplo de captura de uma solicitação de acesso que não inclui o atributo Autenticador de mensagem:



Criptografar com TLS/IPSec

A solução de longo prazo mais eficaz para proteger o RADIUS é criptografar o tráfego entre o servidor RADIUS e o NAD. Isso acrescenta privacidade e uma integridade criptográfica mais forte do que simplesmente contar com o Autenticador de Mensagens derivado do MD5-HMAC. Que, se qualquer um deles puder ser usado entre o servidor RADIUS e o NAD, dependerá de ambos os lados que suportam o método de criptografia.

Os termos gerais usados em toda a indústria para a criptografia TLS do RADIUS são:

- "RadSec" - refere-se ao RFC 6614
- "TLS RadSec" - refere-se ao RFC 6614
- "DTLS RadSec" - refere-se ao RFC 7360

É importante distribuir a criptografia de maneira controlada, pois há sobrecarga de desempenho para a criptografia TLS, bem como considerações sobre o gerenciamento de certificados. Os certificados também terão de ser renovados regularmente.

RADIUS sobre DTLS

O Datagram Transport Layer Security (DTLS) como uma camada de transporte para o RADIUS é definido pelo RFC 7360 que usa certificados para autenticar mutuamente o servidor RADIUS e o NAD criptografa o pacote RADIUS completo usando um túnel TLS. O método de transporte permanece UDP e requer que os certificados sejam implantados no servidor RADIUS e no NAD. Tenha em mente que, ao implantar RADIUS sobre DTLS, é imperativo que a expiração e a substituição de certificados sejam gerenciadas de perto para evitar que certificados expirados interrompam a comunicação RADIUS. O ISE suporta DTLS para comunicação ISE para NAD, já que o ISE 3.4 Radius sobre DTLS não é suportado para RADIUS-Proxy ou RADIUS Token Servers. O RADIUS sobre DTLS também é suportado por muitos dispositivos Cisco que atuam como NADs, como switches e controladores sem fio que executam o IOS-XE®.

RADIUS sobre TLS

A Criptografia TLS (Transport Layer Security) para RADIUS é definida pelo RFC 6614, altera o transporte para TCP e usa TLS para criptografar totalmente os pacotes RADIUS. Isso é comumente usado pelo serviço eduroam como um exemplo. A partir do ISE 3.4, o RADIUS sobre TLS não é suportado, mas é suportado por muitos dispositivos Cisco que atuam como NADs, como switches e controladores sem fio que executam o IOS-XE.

IPSec

O Identity Services Engine tem suporte nativo para túneis IPSec entre ISE e NADs que também suportam túneis IPSec de terminação. Essa é uma boa opção onde o RADIUS sobre DTLS ou o RADIUS sobre TLS não são suportados, mas devem ser usados moderadamente, pois somente 150 túneis são suportados por nó de serviços de política do ISE. O ISE 3.3 e posterior não exige mais uma licença para IPSec, agora está disponível de forma nativa.

Mitigação parcial

Segmentação RADIUS

Segmente o tráfego RADIUS para VLANs de gerenciamento e links criptografados seguros, como pode ser fornecido via SD-WAN ou MACSec. Essa estratégia não elimina o risco do ataque, mas pode reduzir consideravelmente a superfície de ataque da vulnerabilidade. Isso pode ser uma boa medida de intervalo de parada, enquanto os produtos implementam o requisito Message-Authenticator ou o suporte DTLS/RadSec. A exploração exige que um invasor consiga usar a comunicação RADIUS com êxito como MITM (Man-in-the-Middle), de modo que, se um invasor não conseguir entrar em um segmento de rede com esse tráfego, o ataque não será possível. O motivo disso ser apenas uma mitigação parcial é que uma configuração incorreta da rede ou o comprometimento de uma parte da rede pode expor o tráfego RADIUS.

Se o tráfego RADIUS não puder ser segmentado ou criptografado, recursos adicionais podem ser implementados para impedir o MITM bem-sucedido em segmentos de risco como: IP Source Guard, Dynamic ARP Inspection e DHCP Snooping. Também pode ser possível utilizar outros métodos de autenticação baseados no tipo de fluxo de autenticação, como TACACS+, SAML, LDAPS, etc...

Status de vulnerabilidade do Identity Services Engine

As tabelas a seguir descrevem o que está disponível a partir do ISE 3.4 para tornar os fluxos de autenticação protegidos contra Blast-RADIUS. Para recapitular, os 3 itens a seguir devem estar no lugar de um fluxo que utiliza apenas o Autenticador de Mensagem e não a criptografia DTLS/RadSec/IPSec, para que o fluxo não seja vulnerável:
1) O dispositivo de acesso à rede DEVE enviar o atributo Message-Authenticator na solicitação de acesso.

2) O servidor RADIUS DEVE exigir o atributo Message-Authenticator na solicitação de acesso.

3) O servidor RADIUS DEVE responder com o atributo Message-Authenticator nos campos Access-Challenge, Access-Accept e Access-Reject.

Consulte o CSCwk6747, que monitora as alterações para fechar as vulnerabilidades quando o ISE está atuando como cliente RADIUS.

ISE como um 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 um 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.