Atténuation de l'usurpation de protocole Blast-RADIUS (CVE-2024-3596)

Table des matières

Introduction

Le 7 juillet 2024, des chercheurs en sécurité ont révélé la vulnérabilité suivante dans le protocole RADIUS: CVE-2024-3596: Le protocole RADIUS sous RFC 2865 est susceptible d'attaques de falsification par un attaquant sur le chemin qui peut modifier n'importe quelle réponse valide (Access-Accept, Access-Reject, ou Access-Challenge) à n'importe quelle autre réponse en utilisant une attaque de collision à préfixe choisi contre la signature MD5 Response Authenticator. Ils ont publié un document détaillant leurs résultats à l'adresse https://www.blastradius.fail/pdf/radius.pdf qui démontre une falsification de réponse réussie contre les flux qui n'utilisent pas l'attribut Message-Authenticator.

Pour obtenir une liste à jour des produits Cisco affectés par cette vulnérabilité et des versions contenant des correctifs, consultez le site : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. Cet article traite des techniques générales d'atténuation et de leur application à certains produits Cisco, mais pas à tous. Pour plus d'informations, consultez la documentation de chaque produit. En tant que serveur RADIUS phare de Cisco, Identity Service Engine sera traité plus en détail.

Fond

Cette attaque tire parti d'une attaque à préfixe choisi MD5 utilisant des collisions dans MD5, ce qui permet à un attaquant d'ajouter des données supplémentaires au paquet de réponse RADIUS tout en modifiant les attributs existants du paquet de réponse. Un exemple démontré a été la capacité de changer un RADIUS Access-Reject en un RADIUS Access-Accept. Cela est possible parce que RADIUS par défaut n'inclut pas de hachage de tous les attributs dans le paquet. Le document RFC 2869 ajoute l'attribut Message-Authenticator, mais il n'est actuellement requis que pour l'utilisation des protocoles EAP, ce qui signifie que l'attaque décrite dans CVE-2024-3596 est possible contre tout échange non-EAP où le client RADIUS (NAD) n'inclut pas l'attribut Message-Authenticator.

Atténuation

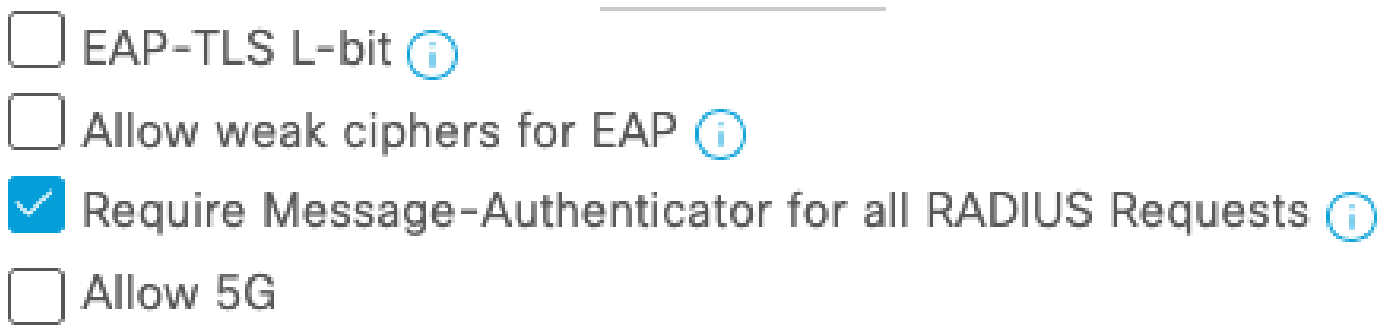
Authentificateur De Message

1) Le client RADIUS doit inclure l'attribut Message-Authenticator.

Lorsque le périphérique d'accès réseau (NAD) inclut l'attribut Message-Authenticator dans la demande d'accès, Identity Services Engine inclut Message-Authenticator dans le paquet Access-Accept, Access-Challenge ou Access-Reject résultant dans toutes les versions.

2) Le serveur RADIUS doit imposer la réception de l'attribut Message-Authenticator.

Il ne suffit pas d'inclure l'authentificateur de message dans la demande d'accès, car l'attaque permet de supprimer l'authentificateur de message de la demande d'accès avant qu'elle ne soit transférée au serveur RADIUS. Le serveur RADIUS doit également exiger que le NAD inclue Message-Authenticator dans la demande d'accès. Ce n'est pas la valeur par défaut sur Identity Services Engine, mais elle peut être activée au niveau des protocoles autorisés, qui s'applique au niveau du jeu de stratégies. L'option sous la configuration des protocoles autorisés est "Require Message-Authenticator" pour toutes les requêtes RADIUS" :



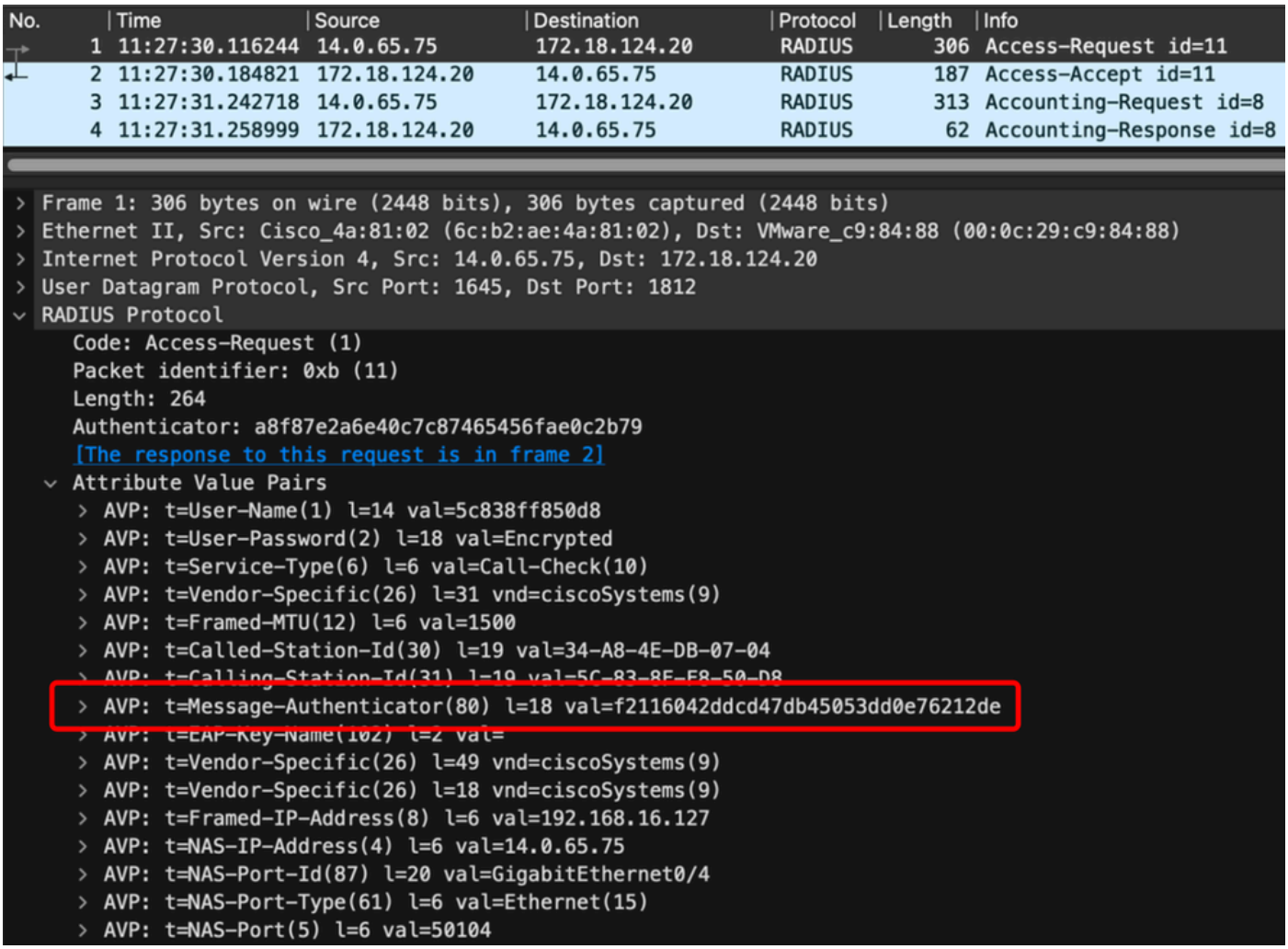
Option Protocoles autorisés dans Identity Services Engine

Les authentifications qui correspondent à un ensemble de stratégies où la configuration des protocoles autorisés nécessite Message-Authenticator, mais où la demande d'accès ne contient pas l'attribut Message-Authenticator seront abandonnées par ISE :

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

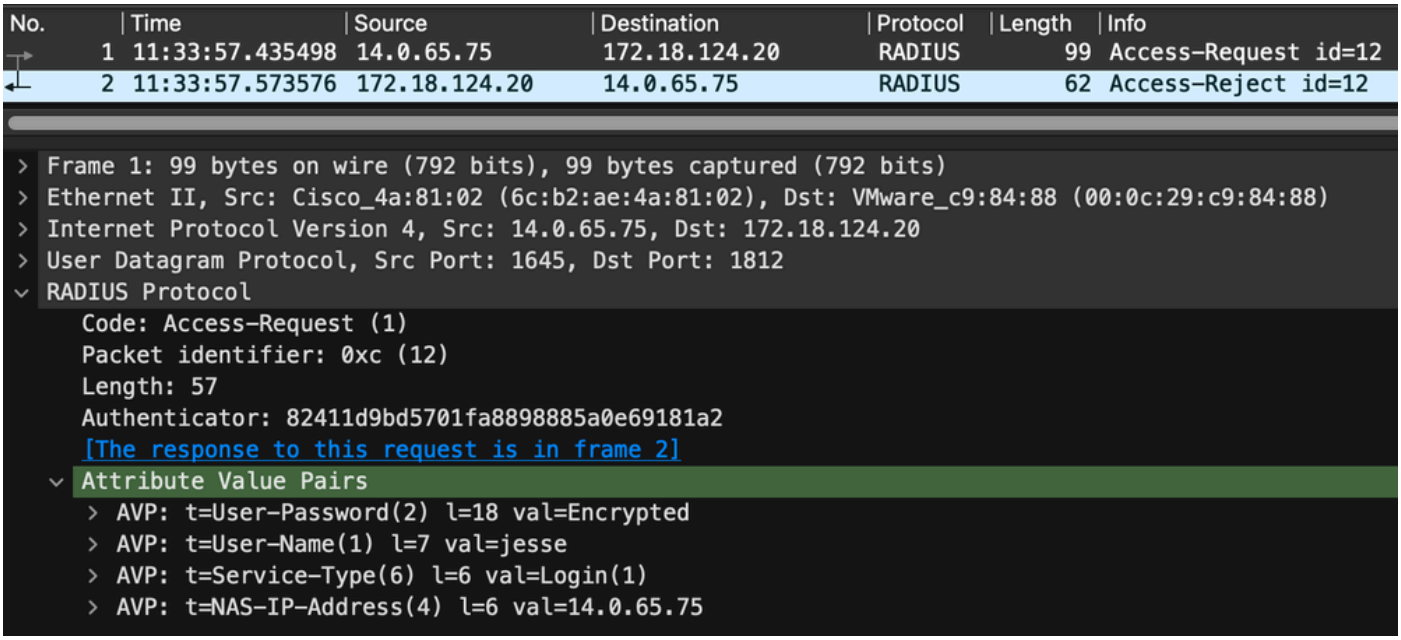
Il est important de vérifier si le NAD envoie Message-Authenticator avant d'être requis par le serveur RADIUS car il ne s'agit pas d'un attribut négocié, il appartient au NAD de l'envoyer par défaut ou d'être configuré pour l'envoyer. Message-Authenticator n'est pas l'un des attributs signalés par ISE, une capture de paquets est la meilleure façon de déterminer si un NAD/Cas d'utilisation inclut Message-Authenticator. ISE intègre une fonctionnalité de capture de paquets sous Opérations -> Dépannage -> Outils de diagnostic -> Outils généraux -> Dépôt TCP. Gardez à l'esprit que différents cas d'utilisation du même NAD peuvent inclure ou non Message-Authenticator.

Voici un exemple de capture d'une demande d'accès qui inclut l'attribut Message-Authenticator :



Attribut Message-authenticator dans la requête d'accès Radius

L'exemple suivant est un exemple de capture d'une demande d'accès qui n'inclut pas l'attribut Message-Authenticator :



Chiffrement avec TLS/IPSec

La solution à long terme la plus efficace pour sécuriser RADIUS consiste à chiffrer le trafic entre le serveur RADIUS et le NAD. Ceci ajoute à la fois la confidentialité et une intégrité cryptographique plus forte que le simple fait de se fier à l'authentificateur de message dérivé de MD5-HMAC. Si l'un de ces éléments peut être utilisé entre le serveur RADIUS et le NAD, cela dépend de la prise en charge de la méthode de cryptage par les deux parties.

Les termes généraux utilisés dans le secteur pour le chiffrement TLS de RADIUS sont les suivants :

- « RadSec » - fait référence à la norme RFC 6614
- « RadSec TLS » - fait référence à RFC 6614
- « RadSec DTLS » - fait référence à RFC 7360

Il est important de déployer le chiffrement de manière contrôlée, car le chiffrement TLS et la gestion des certificats entraînent une baisse des performances. Les certificats devront également être renouvelés sur une base régulière.

RADIUS sur DTLS

Le protocole DTLS (Datagram Transport Layer Security) en tant que couche de transport pour RADIUS est défini par la RFC 7360 qui utilise des certificats pour authentifier mutuellement le serveur RADIUS et le NAD chiffre ensuite le paquet RADIUS complet à l'aide d'un tunnel TLS. La méthode de transport reste UDP et nécessite le déploiement de certificats sur le serveur RADIUS et NAD. Gardez à l'esprit que lors du déploiement de RADIUS sur DTLS, il est impératif que l'expiration et le remplacement des certificats soient étroitement gérés pour empêcher les certificats expirés d'interrompre la communication RADIUS. ISE prend en charge DTLS pour les communications ISE à NAD, car à partir de la version ISE 3.4, Radius sur DTLS n'est pas pris en charge pour les serveurs proxy RADIUS ou les serveurs à jetons RADIUS. RADIUS sur DTLS est également pris en charge par de nombreux périphériques Cisco qui agissent en tant que NAD, tels que des commutateurs et des contrôleurs sans fil exécutant IOS-XE®.

RADIUS sur TLS

Le chiffrement TLS (Transport Layer Security) pour RADIUS est défini par la RFC 6614, modifie le transport en TCP et utilise TLS pour chiffrer entièrement les paquets RADIUS. C'est un exemple couramment utilisé par le service eduroam. Depuis ISE 3.4, RADIUS sur TLS n'est pas pris en charge, mais il est pris en charge par de nombreux périphériques Cisco qui agissent en tant que NAD, tels que des commutateurs et des contrôleurs sans fil exécutant IOS-XE.

IPSEC

Identity Services Engine prend en charge de manière native les tunnels IPSec entre ISE et NAD, qui prennent également en charge les tunnels IPSec de fin. Il s'agit d'une bonne option où RADIUS sur DTLS ou RADIUS sur TLS n'est pas pris en charge, mais doit être utilisé avec parcimonie, car seuls 150 tunnels sont pris en charge par noeud de services de stratégie ISE. ISE 3.3 et versions ultérieures n'exige plus de licence pour IPSec ; elle est désormais disponible en mode natif.

Atténuation partielle

Segmentation RADIUS

Segmenter le trafic RADIUS vers les VLAN de gestion et les liaisons chiffrées sécurisées, telles que celles fournies via SD-WAN ou MACSec. Cette stratégie ne réduit pas le risque d'attaque à zéro, mais peut réduire considérablement la surface d'attaque de la vulnérabilité. Il peut s'agir d'une bonne mesure d'interruption pendant que les produits déploient la configuration requise pour Message-Authenticator ou la prise en charge DTLS/RadSec. L'attaque nécessite qu'un pirate réussisse à faire fonctionner la communication RADIUS avec le mode « Man-in-the-Middle » (MITM). Ainsi, si un pirate ne parvient pas à accéder à un segment de réseau avec ce trafic, l'attaque n'est pas possible. La raison pour laquelle ce problème n'est qu'une atténuation partielle est qu'une configuration incorrecte ou une compromission d'une partie du réseau peut exposer le trafic RADIUS.

Si le trafic RADIUS ne peut pas être segmenté ou chiffré, des fonctionnalités supplémentaires peuvent être implémentées pour empêcher la réussite de la MITM sur les segments à risque tels que : IP Source Guard, Dynamic ARP Inspection et DHCP Snooping. Il peut également être possible d'utiliser d'autres méthodes d'authentification basées sur le type de flux d'authentification comme TACACS+, SAML, LDAPS, etc...

État de vulnérabilité Identity Services Engine

Les tableaux ci-dessous décrivent les éléments disponibles dans ISE 3.4 pour protéger les flux d'authentification contre Blast-RADIUS. Pour récapituler, les 3 éléments suivants doivent être en cours pour un flux utilisant uniquement Message-Authenticator et non le chiffrement DTLS/RadSec/IPSec, pour que le flux ne soit pas vulnérable :
1) Le périphérique d'accès réseau DOIT envoyer l'attribut Message-Authenticator dans la requête d'accès.

2) Le serveur RADIUS DOIT exiger l'attribut Message-Authenticator dans la demande d'accès.

3) Le serveur RADIUS DOIT répondre avec l'attribut Message-Authenticator dans Access-Challenge, Access-Accept et Access-Reject.

Reportez-vous au document CSCwk67747 qui suit les modifications pour fermer les vulnérabilités lorsque ISE agit en tant que client RADIUS.

ISE comme serveur 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 comme client 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.