BlastRADIUS (CVE-2024-3596) Protocol Spoofing-Eindämmung

Inhalt

Einleitung

Am 7. Juli 2024 enthüllten Sicherheitsforscher die folgende Schwachstelle im RADIUS-Protokoll: CVE-2024-3596: Das RADIUS-Protokoll unter RFC 2865 ist anfällig für Fälschungsangriffe eines On-Path-Angreifers, der jede gültige Antwort (Access-Accept, Access-Reject oder Access-Challenge) auf eine andere Antwort ändern kann mithilfe eines "selected-prefix"-Kollisionsangriffs auf die MD5 Response Authenticator-Signatur. Sie haben einen Bericht veröffentlicht, in dem sie ihre Ergebnisse unter https://www.blastradius.fail/pdf/radius.pdf ausführlich darlegen, was eine erfolgreiche Fälschung von Reaktionen auf Datenflüsse zeigt, die das Message-Authenticator-Attribut nicht verwenden.

Eine aktuelle Liste der von dieser Sicherheitslücke betroffenen Cisco Produkte und der Versionen mit Patches finden Sie unter: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. Dieser Artikel behandelt allgemeine Eindämmungstechniken sowie deren Anwendung auf einige, jedoch nicht alle Cisco Produkte. Nähere Informationen finden Sie in der jeweiligen Produktdokumentation. Als RADIUS-Server, das Flaggschiff von Cisco, wird Identity Service Engine genauer behandelt.

Hintergrund

Dieser Angriff nutzt einen MD5-Selected-Prefix-Angriff, bei dem Kollisionen in MD5 verwendet werden, wodurch ein Angreifer dem RADIUS-Antwortpaket zusätzliche Daten hinzufügen und gleichzeitig vorhandene Attribute des Antwortpakets ändern kann. Ein Beispiel hierfür war die Möglichkeit, eine RADIUS Access-Reject in eine RADIUS Access-Accept zu ändern. Dies ist möglich, da RADIUS standardmäßig keinen Hash aller Attribute im Paket enthält. RFC 2869 fügt das Message-Authenticator-Attribut hinzu, es muss jedoch derzeit nur bei Verwendung von EAP-Protokollen eingeschlossen werden. Dies bedeutet, dass der in CVE-2024-3596 beschriebene Angriff gegen jeden Nicht-EAP-Austausch möglich ist, bei dem der RADIUS-Client (NAD) das Message-Authenticator-Attribut nicht enthält.

Eindämmung

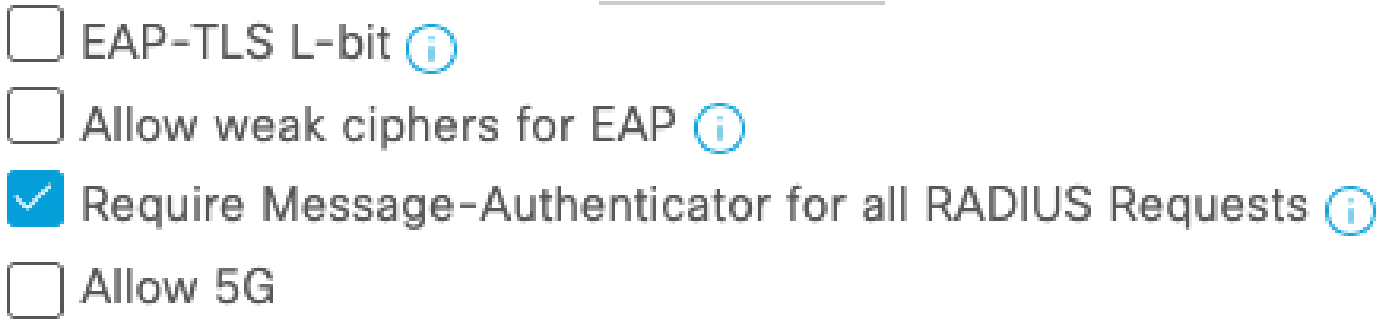
Message-Authenticator

1) Der RADIUS-Client muss das Message-Authenticator-Attribut enthalten.

Wenn das Netzwerkzugriffsgerät (NAD) das Message-Authenticator-Attribut in die Access-Request einbindet, nimmt die Identity Services Engine Message-Authenticator in das resultierende Access-Accept-, Access-Challenge- oder Access-Reject-Paket in allen Versionen auf.

2) Der RADIUS-Server muss den Empfang des Message-Authenticator-Attributs erzwingen.

Es reicht nicht aus, nur den Message-Authenticator in die Access-Request einzubeziehen, da der Angriff es ermöglicht, den Message-Authenticator aus der Access-Request zu entfernen, bevor er an den RADIUS-Server weitergeleitet wird. Außerdem muss der RADIUS-Server vom NAD verlangen, dass Message-Authenticator in die Access-Request aufgenommen wird. Dies ist nicht die Standardeinstellung für die Identity Services Engine, kann jedoch auf der Ebene der zulässigen Protokolle aktiviert werden, die auf der Ebene des Richtliniensatzes angewendet wird. Die Option unter der Konfiguration für zulässige Protokolle lautet "Message-Authenticator anfordern" für alle RADIUS-Anfragen:



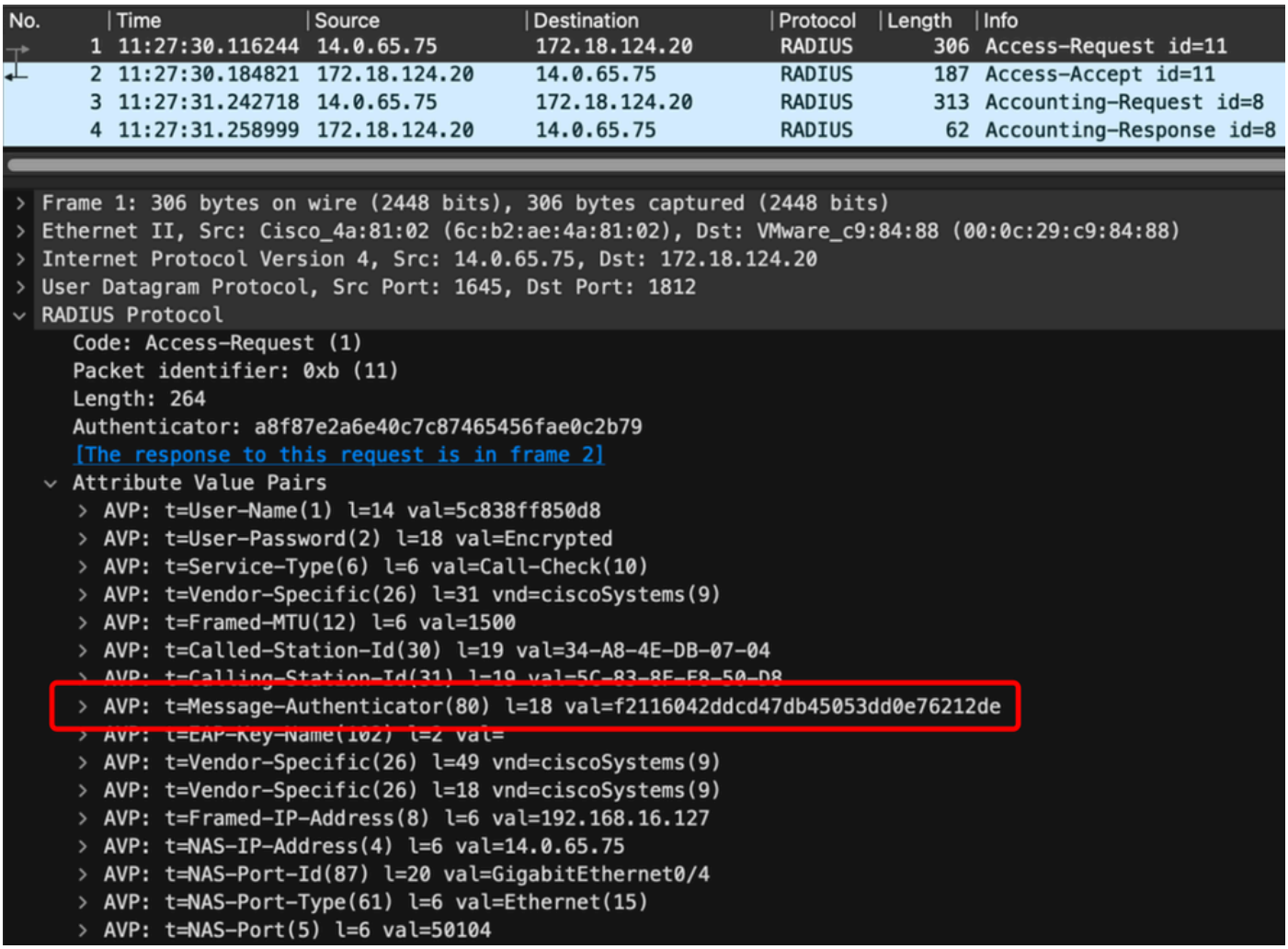
Option für zulässige Protokolle in Identity Services Engine

Authentifizierungen, die einem Richtliniensatz entsprechen, bei dem die Konfiguration für zulässige Protokolle Message-Authenticator erfordert, die Access-Request jedoch das Message-Authenticator-Attribut nicht enthält, werden von ISE gelöscht:

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

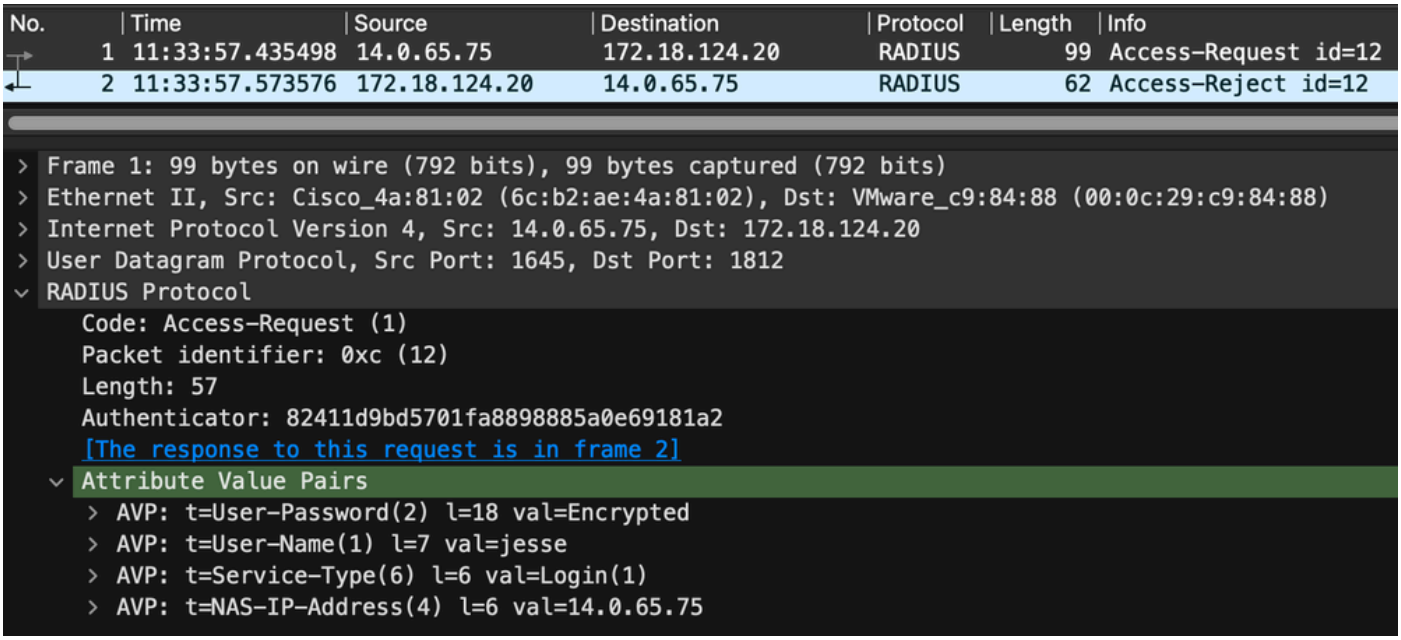
Es ist wichtig, zu überprüfen, ob der NAD Message Authenticator sendet, bevor er vom RADIUS-Server benötigt wird, da es sich nicht um ein ausgehandeltes Attribut handelt. Es ist Sache des NAD, dieses entweder standardmäßig zu senden oder so konfiguriert zu sein, dass es gesendet wird. Message-Authenticator ist keines der Attribute, die von der ISE gemeldet werden. Eine Paketerfassung ist die beste Methode, um zu bestimmen, ob ein NAD/Anwendungsfall Message-Authenticator enthält. Die ISE verfügt über eine integrierte Paketerfassungsfunktion unter Operationen -> Fehlerbehebung -> Diagnosetools -> Allgemeine Tools -> TCP-Dump. Beachten Sie, dass unterschiedliche Anwendungsfälle von derselben NAD entweder Message-Authenticator enthalten oder nicht enthalten können.

Im Folgenden finden Sie ein Beispiel für die Erfassung einer Access-Request, die das Message-Authenticator-Attribut enthält:



Message-Authenticator-Attribut in Radius-Zugriffsanforderung

Im folgenden Beispiel wird eine Access-Request erfasst, die das Message-Authenticator-Attribut nicht enthält:



Verschlüsseln mit TLS/IPSec

Die effektivste langfristige Lösung zur Sicherung von RADIUS besteht in der Verschlüsselung des Datenverkehrs zwischen dem RADIUS-Server und dem NAD. Dadurch wird sowohl Datenschutz als auch kryptografische Integrität gewährleistet, da Sie sich nicht nur auf den MD5-HMAC Message-Authenticator verlassen müssen. Welche dieser Optionen zwischen dem RADIUS-Server und der NAD verwendet werden können, hängt davon ab, dass beide Seiten die Verschlüsselungsmethode unterstützen.

Branchenweit werden für die TLS-Verschlüsselung von RADIUS folgende Begriffe verwendet:

- "RadSec" - bezieht sich auf RFC 6614
- "RadSec TLS" - bezieht sich auf RFC 6614
- "RadSec DTLS" - bezieht sich auf RFC 7360

Es ist wichtig, die Verschlüsselung kontrolliert einzuführen, da die TLS-Verschlüsselung einen Performance-Overhead verursacht und das Zertifikatsmanagement berücksichtigt wird. Auch die Zertifikate müssen regelmäßig erneuert werden.

RADIUS über DTLS

Datagram Transport Layer Security (DTLS) als Transport Layer für RADIUS wird durch RFC 7360 definiert, das Zertifikate für die gegenseitige Authentifizierung des RADIUS-Servers verwendet, und der NAD verschlüsselt dann das vollständige RADIUS-Paket mithilfe eines TLS-Tunnels. Die Transportmethode bleibt UDP und erfordert die Bereitstellung von Zertifikaten sowohl auf dem RADIUS-Server als auch auf NAD. Beachten Sie, dass bei der Bereitstellung von RADIUS über DTLS das Ablaufdatum und der Austausch von Zertifikaten eng verwaltet werden müssen, damit abgelaufene Zertifikate die RADIUS-Kommunikation nicht unterbrechen. Die ISE unterstützt DTLS für die Kommunikation zwischen ISE und NAD, da der Radius über DTLS für ISE 3.4 für RADIUS-Proxy- oder RADIUS-Token-Server nicht unterstützt wird. RADIUS über DTLS wird auch von vielen Cisco Geräten unterstützt, die als NADs fungieren, z. B. Switches und Wireless-Controller, auf denen IOS-XE® ausgeführt wird.

RADIUS über TLS

Transport Layer Security (TLS) Encryption for RADIUS wird von RFC 6614 definiert, ändert den Transport zu TCP und verwendet TLS zur vollständigen Verschlüsselung von RADIUS-Paketen. Dies wird vom eduroam-Dienst häufig als Beispiel verwendet. Ab ISE 3.4 wird RADIUS over TLS nicht mehr unterstützt, jedoch von vielen Cisco Geräten, die als NADs fungieren, wie Switches und Wireless-Controller, auf denen IOS-XE ausgeführt wird.

IPsec

Identity Services Engine bietet native Unterstützung für IPSec-Tunnel zwischen ISE und NADs, die auch terminierende IPSec-Tunnel unterstützen. Dies ist eine gute Option, wenn RADIUS über DTLS oder RADIUS über TLS nicht unterstützt wird, jedoch nur sparsam verwendet werden sollte, da pro ISE Policy Services Node nur 150 Tunnel unterstützt werden. ISE 3.3 und höher erfordern keine Lizenz für IPSec mehr. Sie ist jetzt nativ verfügbar.

Teilweise Eindämmung

RADIUS-Segmentierung

Segmentierung des RADIUS-Datenverkehrs in Management-VLANs und sichere, verschlüsselte Verbindungen, wie sie über SD-WAN oder MACSec bereitgestellt werden können Diese Strategie bringt das Risiko des Angriffs nicht auf Null, kann jedoch die Angriffsfläche der Schwachstelle erheblich verringern. Dies kann eine gute Stopp-Gap-Messgröße sein, wenn Produkte die Message-Authenticator-Anforderung erfüllen oder DTLS/RadSec unterstützen. Der Exploit erfordert, dass ein Angreifer die RADIUS-Kommunikation (Man-in-the-Middle, MITM) erfolgreich durchführt. Wenn ein Angreifer mit diesem Datenverkehr nicht in ein Netzwerksegment gelangen kann, ist der Angriff nicht möglich. Dies ist nur eine teilweise Reduzierung, da der RADIUS-Datenverkehr durch eine falsche Netzwerkkonfiguration oder eine Kompromittierung eines Teils des Netzwerks verfügbar gemacht werden kann.

Wenn der RADIUS-Datenverkehr nicht segmentiert oder verschlüsselt werden kann, können zusätzliche Funktionen implementiert werden, die einen erfolgreichen MITM in Risikosegmenten wie IP Source Guard, Dynamic ARP Inspection und DHCP Snooping verhindern. Es können auch andere Authentifizierungsmethoden auf Basis des Authentifizierungsflusstyps wie TACACS+, SAML, LDAPS usw. verwendet werden.

Schwachstellenstatus der Identity Services Engine

In den folgenden Tabellen wird beschrieben, was ab ISE 3.4 verfügbar ist, um Authentifizierungsflüsse vor Blast-RADIUS zu schützen. Um eine Zusammenfassung zu erstellen, müssen die folgenden drei Elemente für einen Fluss vorhanden sein, der nur Message-Authenticator und keine DTLS/RadSec/IPSec-Verschlüsselung verwendet, damit der Fluss nicht anfällig ist:
1) Das Netzwerkzugriffsgerät MUSS das Message-Authenticator-Attribut in der Access-Request senden.

2) Der RADIUS-Server MUSS das Message-Authenticator-Attribut in der Access-Request benötigen.

3) Der RADIUS-Server MUSS mit dem Message-Authenticator-Attribut in Access-Challenge, Access-Accept und Access-Reject antworten.

Weitere Informationen finden Sie unter CSCwk67747, das die Änderungen nachverfolgt, um die Schwachstellen zu schließen, wenn die ISE als RADIUS-Client agiert.

ISE als RADIUS-Server

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 als RADIUS-Client

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.