Riduzione dello spoofing del protocollo Blast-RADIUS (CVE-2024-3596)

Sommario

Introduzione

Il 7 luglio 2024, i ricercatori di sicurezza hanno rivelato la seguente vulnerabilità nel protocollo RADIUS: CVE-2024-3596: Il protocollo RADIUS in base alla RFC 2865 è suscettibile di attacchi falsificati da parte di un attaccante sul percorso che può modificare qualsiasi risposta valida (Access-Accept, Access-Reject, or Access-Challenge) a qualsiasi altra risposta utilizzando un attacco di collisione a prefisso scelto contro la firma dell'autenticatore di risposta MD5. Hanno pubblicato un documento dettagliato dei risultati su https://www.blastradius.fail/pdf/radius.pdf che dimostra la riuscita della risposta falsificata contro i flussi che non utilizzano l'attributo Message-Authenticator.

Per un elenco aggiornato dei prodotti Cisco interessati da questa vulnerabilità e delle versioni che contengono correzioni, visitare: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3. Questo articolo tratta delle tecniche generali di mitigazione e del modo in cui si applicano ad alcuni prodotti Cisco, ma non a tutti, è necessario consultare la documentazione dei singoli prodotti per le specifiche. In qualità di server RADIUS di punta di Cisco, Identity Service Engine verrà descritto più dettagliatamente.

Introduzione

Questo attacco sfrutta un attacco MD5 basato sul prefisso scelto utilizzando collisioni in MD5, che consente a un utente non autorizzato di aggiungere ulteriori dati al pacchetto di risposta RADIUS modificando al contempo gli attributi esistenti del pacchetto di risposta. È stato dimostrato, ad esempio, che è possibile modificare un rifiuto di accesso RADIUS in un rifiuto di accesso RADIUS. Ciò è possibile perché per impostazione predefinita RADIUS non include un hash di tutti gli attributi nel pacchetto. La RFC 2869 non aggiunge l'attributo Message-Authenticator, ma al momento è necessario includerlo solo quando si utilizzano i protocolli EAP, il che significa che l'attacco descritto in CVE-2024-3596 è possibile contro qualsiasi scambio non EAP in cui il client RADIUS (NAD) non include l'attributo Message-Authenticator.

Attenuazione

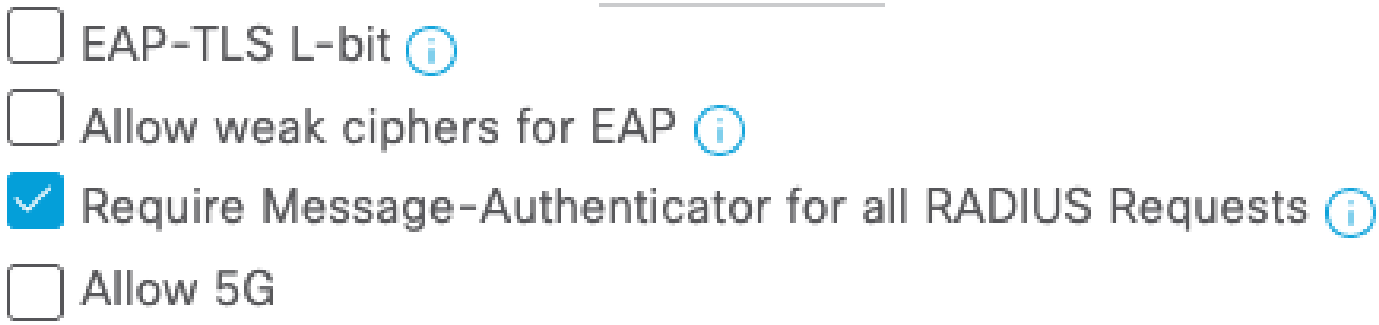
Message-Authenticator

1) Il client RADIUS deve includere l'attributo Message-Authentication.

Quando il dispositivo di accesso alla rete (NAD) include l'attributo Message-Authenticator nel pacchetto Access-Request, Identity Services Engine includerà Message-Authenticator nel pacchetto Access-Accept, Access-Challenge o Access-Reject risultante in tutte le versioni.

2) Il server RADIUS deve imporre la ricezione dell'attributo Message-Authenticator.

Non è sufficiente includere l'autenticatore del messaggio nella richiesta di accesso, in quanto l'attacco consente di rimuovere l'autenticatore del messaggio dalla richiesta di accesso prima che venga inoltrata al server RADIUS. Il server RADIUS deve inoltre richiedere a NAD di includere Message-Authenticator in Access-Request. Non è l'impostazione predefinita su Identity Services Engine, ma può essere abilitata al livello di protocolli consentiti, che si applica al livello di set di criteri. L'opzione nella configurazione Protocolli consentiti è "Richiedi autenticatore messaggio" per tutte le richieste RADIUS":



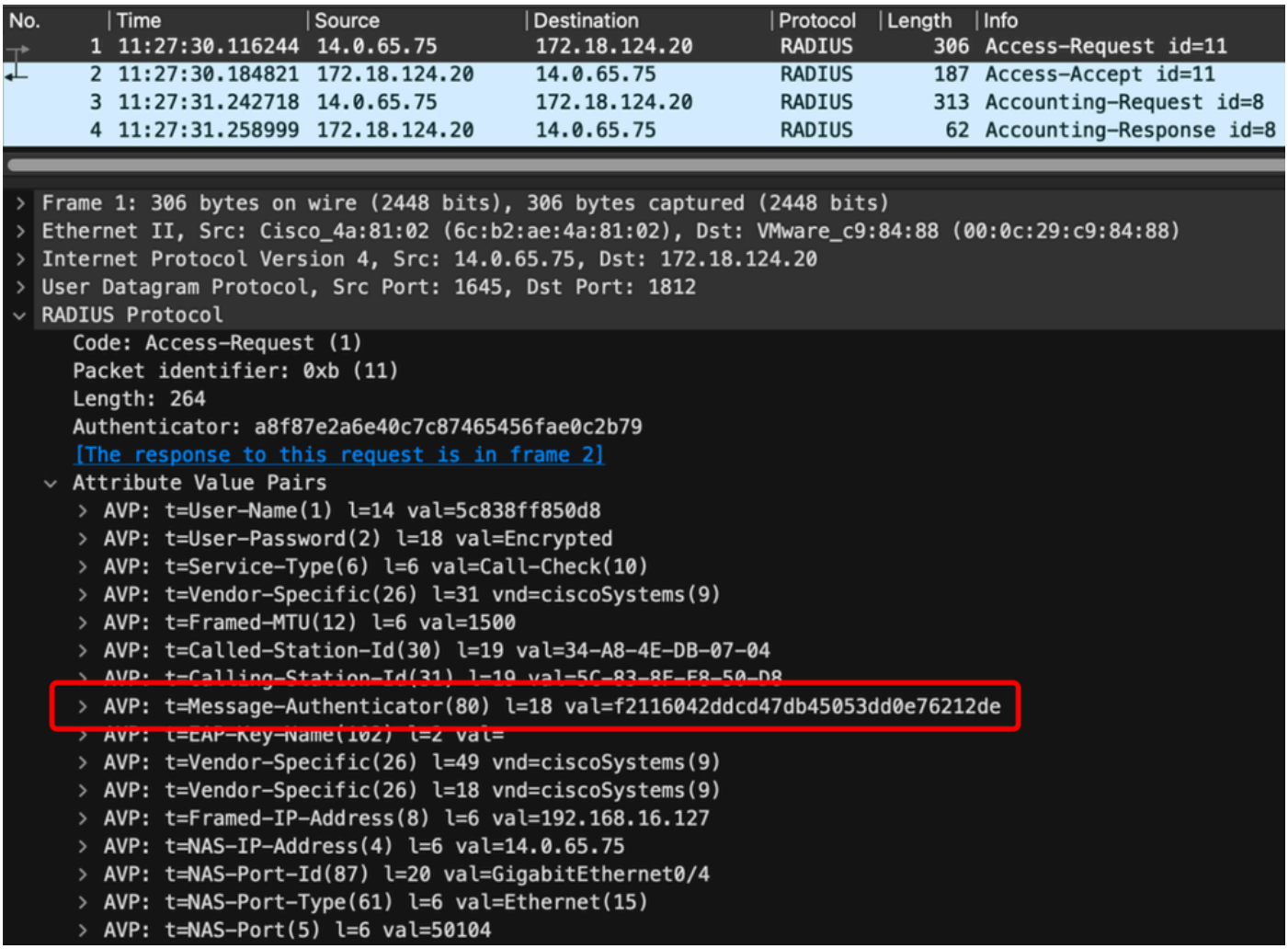
Opzione Protocolli consentiti in Identity Services Engine

Le autenticazioni che corrispondono a un set di criteri in cui la configurazione dei protocolli consentiti richiede Message-Authenticator, ma in cui Access-Request non contiene l'attributo Message-Authenticator verranno eliminate da ISE:

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

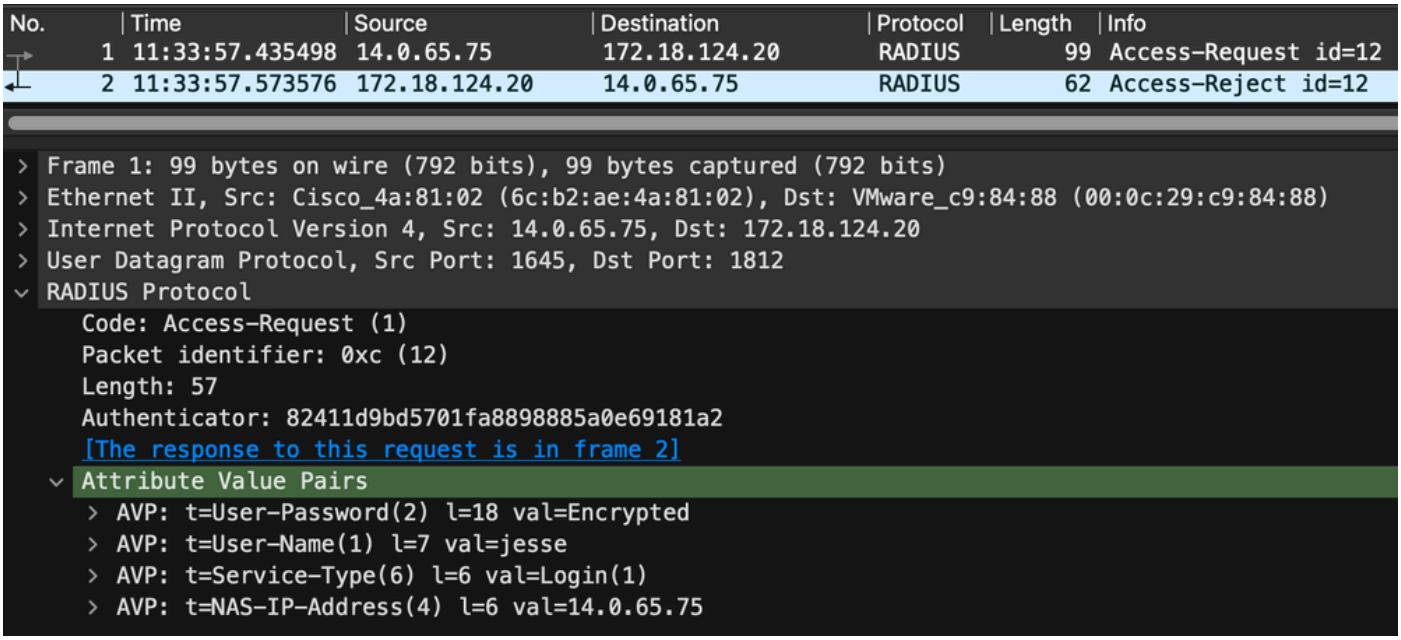
È importante verificare se NAD invia Message-Authenticator prima di essere richiesto dal server RADIUS. Poiché non si tratta di un attributo negoziato, spetta a NAD inviarlo per impostazione predefinita o configurarlo per l'invio. Message-Authenticator non è uno degli attributi riportati da ISE; un packet capture è il modo migliore per determinare se un NAD/Use Case include Message-Authenticator. ISE ha integrato la funzionalità di acquisizione pacchetti in Operations (Operazioni) -> Troubleshoot (Risoluzione problemi) -> Diagnostic Tools (Strumenti diagnostici) -> General Tools (Strumenti generali) -> TCP Dump. Tenere presente che casi di utilizzo diversi dello stesso NAD possono includere o meno l'opzione Message-Authenticator.

Di seguito viene riportato un esempio di acquisizione di una richiesta di accesso che include l'attributo Message-Authenticator:



Attributo message-authenticator in Radius access-request

Di seguito è riportato un esempio di acquisizione di un oggetto Access-Request che non include l'attributo Message-Authenticator:



Crittografia con TLS/IPSec

La soluzione a lungo termine più efficace per proteggere RADIUS è crittografare il traffico tra il server RADIUS e il server NAD. In questo modo viene aggiunta sia la privacy che una maggiore integrità crittografica rispetto all'utilizzo dell'autenticatore di messaggi derivato da MD5-HMAC. Che, se è possibile utilizzare tra il server RADIUS e il server AND, dipende da entrambi i lati che supportano il metodo di crittografia.

I termini utilizzati nel settore per la crittografia TLS di RADIUS sono:

- "RadSec" - si riferisce alla RFC 6614
- "RadSec TLS": si riferisce alla RFC 6614
- "RadSec DTLS": si riferisce alla RFC 7360

È importante implementare la crittografia in modo controllato, in quanto il sovraccarico delle prestazioni per la crittografia TLS e le considerazioni sulla gestione dei certificati sono fattori importanti. Anche i certificati dovranno essere rinnovati regolarmente.

RADIUS over DTLS

DTLS (Datagram Transport Layer Security) come livello di trasporto per RADIUS è definito dalla RFC 7360 che utilizza i certificati per autenticare reciprocamente il server RADIUS e il server NAD, quindi cripta il pacchetto RADIUS completo utilizzando un tunnel TLS. Il metodo di trasporto rimane UDP e richiede la distribuzione di certificati sia nel server RADIUS che in NAD. Tenere presente che quando si distribuisce RADIUS su DTLS, è necessario che la scadenza e la sostituzione dei certificati vengano gestite attentamente per impedire ai certificati scaduti di interrompere la comunicazione RADIUS. ISE supporta DTLS per le comunicazioni da ISE a NAD, in quanto ISE 3.4 Radius over DTLS non è supportato per i server proxy RADIUS o i server token RADIUS. RADIUS over DTLS è supportato anche da molti dispositivi Cisco che fungono da servizi di rilevamento di virus (NAD), quali switch e controller wireless con IOS-XE®.

RADIUS over TLS

La crittografia TLS (Transport Layer Security) per RADIUS è definita dalla RFC 6614, imposta il trasporto su TCP e usa TLS per crittografare completamente i pacchetti RADIUS. Questo è comunemente usato dal servizio eduroam come esempio. A partire dalla versione ISE 3.4, RADIUS over TLS non è supportato, ma è supportato da molti dispositivi Cisco che agiscono come NAD, ad esempio switch e controller wireless con IOS-XE.

IPSec

Identity Services Engine dispone di supporto nativo per i tunnel IPSec tra ISE e NAD, che supportano anche la terminazione dei tunnel IPSec. Questa è una buona opzione quando RADIUS over DTLS o RADIUS over TLS non è supportato, ma deve essere usato con moderazione, in quanto solo 150 tunnel sono supportati per ISE Policy Services Node. ISE 3.3 e versioni successive non richiedono più una licenza per IPSec, ma sono ora disponibili in modalità nativa.

Riduzione parziale

Segmentazione RADIUS

Segmentare il traffico RADIUS verso le VLAN di gestione e i collegamenti protetti e crittografati, ad esempio tramite SD-WAN o MACSec. Questa strategia non azzera il rischio di attacco ma può ridurre notevolmente la superficie di attacco della vulnerabilità. Ciò può costituire una buona misura di interruzione durante l'implementazione del requisito Message-Authenticator o del supporto DTLS/RadSec. L'attacco richiede che l'autore di un attacco riesca a gestire con successo la comunicazione RADIUS (Man-in-the-Middle, MITM) in modo che se l'autore di un attacco non riesce ad accedere a un segmento di rete con quel traffico, l'attacco non è possibile. Questa limitazione è solo parziale in quanto una configurazione errata o il danneggiamento di una parte della rete può esporre il traffico RADIUS.

Se il traffico RADIUS non può essere segmentato o criptato, è possibile implementare funzionalità aggiuntive per impedire il corretto funzionamento del protocollo MITM su segmenti a rischio, quali: IP Source Guard, Dynamic ARP Inspection e Snooping DHCP. Può essere inoltre possibile utilizzare altri metodi di autenticazione basati sul tipo di flusso di autenticazione, ad esempio TACACS+, SAML, LDAPS, ecc.

Stato vulnerabilità Identity Services Engine

Nelle tabelle seguenti vengono descritti i dati disponibili a partire da ISE 3.4 per proteggere i flussi di autenticazione da Blast-RADIUS. Affinché il flusso non sia vulnerabile, per un flusso che utilizza solo l'autenticatore del messaggio e non la crittografia DTLS/RadSec/IPSec è necessario che siano presenti i tre elementi seguenti:
1) Il dispositivo di accesso alla rete DEVE inviare l'attributo Message-Authenticator in Access-Request.

2) Il server RADIUS DEVE richiedere l'attributo Message-Authenticator in Access-Request.

3) Il server RADIUS DEVE rispondere con l'attributo Message-Authenticator in Access-Challenge, Access-Accept e Access-Reject.

Fare riferimento a CSCwk67747 per verificare le modifiche e chiudere le vulnerabilità quando ISE agisce come client RADIUS.

ISE come server 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 come 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).