Consigli per evitare attacchi con spray di password mirati ai servizi VPN ad accesso remoto in un firewall sicuro

Sommario

Introduzione

In questo documento vengono forniti suggerimenti da prendere in considerazione per evitare attacchi con spray di password destinati ai servizi VPN ad accesso remoto in Secure Firewall.

Premesse

Gli attacchi tramite spray di password sono un tipo di attacco di forza bruta in cui un utente malintenzionato tenta di ottenere l'accesso non autorizzato a più account utente provando sistematicamente alcune password comunemente utilizzate in molti account. Gli attacchi tramite spray di password riusciti possono comportare l'accesso non autorizzato a informazioni riservate, violazioni dei dati e potenziali compromessi dell'integrità della rete

Inoltre, questi attacchi, anche quando non riescono a ottenere l'accesso, possono consumare le risorse computazionali dal Secure Firewall e impedire agli utenti validi di connettersi ai servizi VPN di accesso remoto.

Comportamenti osservati

Quando il firewall protetto è bersaglio di attacchi con spray di password nei servizi VPN ad accesso remoto, è possibile identificare questi attacchi monitorando i syslog e utilizzando comandi show specifici. I comportamenti più comuni da cercare includono:

Importo insolito di richieste di autenticazione rifiutate

L'headend VPN Cisco Secure Firewall ASA o FTD mostra i sintomi di attacchi con spray di password con una frequenza insolita (100-migliaia o milioni) di tentativi di autenticazione rifiutati.

Nota: questi tentativi di autenticazione insoliti possono essere indirizzati al database LOCALE o ai server di autenticazione esterni.

Il modo migliore per rilevarlo è guardando il syslog. Cercare un numero insolito di uno qualsiasi dei successivi ID syslog ASA:

- %ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database :

user

= *admin* : user

IP

= *x.x.x.x*

- %ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

- %ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.

Il nome utente è sempre nascosto finché non si configura il comando no logging hide username sull'appliance ASA.

Nota: questo fornisce informazioni dettagliate per verificare se gli utenti validi sono generati o conosciuti da IP offensivi. Tuttavia, si prega di essere cauti, in quanto i nomi utente saranno visibili nei log.

Per verificare, accedere all'interfaccia della riga di comando (CLI) ASA o FTD, eseguire il comando show aaa-server e verificare la presenza di un numero insolito di richieste di autenticazione tentate e rifiutate su uno dei server AAA configurati:

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against external server
Server Protocol: ldap
Server Hostname: ldap-server.example.com
Server Address: 10.10.10.10
Server port: 636
Server status: ACTIVE, Last transaction at unknown
Number of pending requests 0
Average round trip time 0ms
```

Number of authentication requests 2228536 - - - - - >>>> Unusual increments

```
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 1312
```

Number of rejects 2225363 - - - - - >>>> Unusual increments / Unusual rejection rate

```
Number of challenges 0
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 1
```

```
Number of unrecognized responses 0
```

Consigli

Prendere in considerazione e applicare le raccomandazioni successive.

1. Abilitare la registrazione.

La registrazione è una parte cruciale della sicurezza informatica che comporta la registrazione degli eventi che si verificano all'interno di un sistema. L'assenza di registri dettagliati lascia delle lacune nella comprensione, ostacolando una chiara analisi del metodo di attacco. Si consiglia di abilitare la registrazione su un server syslog remoto per migliorare la correlazione e il controllo degli incidenti di rete e di sicurezza tra vari dispositivi di rete.

Per informazioni su come configurare la registrazione, vedere le seguenti guide specifiche della piattaforma:

Software Cisco ASA:

- Guida all'uso di Secure ASA Firewall
- Capitolo Logging della guida alla configurazione della CLI per le operazioni generali di Cisco Secure Firewall serie ASA

Software Cisco FTD:

- Configurare la registrazione su FTD tramite Centro gestione firewall
- Sezione Configure Syslog nel capitolo Platform Settings della Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center
- Configurazione e verifica di Syslog in Gestione periferiche di Firepower
- Sezione Configurazione delle impostazioni di registrazione del sistema nel capitolo System Settings della Guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager

---

Nota: gli ID dei messaggi syslog necessari per verificare i comportamenti descritti in questo documento (113015, 113005 e 716039) devono essere abilitati a livello informativo (6). Questi ID rientrano nelle classi di registrazione 'auth' e 'webvpn'.

---

2. Configurare le funzionalità di rilevamento delle minacce o le misure di protezione

avanzata per la VPN ad accesso remoto.

Per ridurre l'impatto e la probabilità che si verifichino questi attacchi di forza bruta sulle connessioni RAVPN, è possibile esaminare e applicare le opzioni di configurazione successive:

Opzione 1 (preferita): configurare il rilevamento delle minacce per i servizi VPN di accesso remoto.

Le funzionalità di rilevamento delle minacce per i servizi VPN ad accesso remoto consentono di proteggere da questi tipi di attacchi bloccando automaticamente l'host (indirizzo IP) che supera le soglie configurate, in modo da impedire ulteriori tentativi finché non si rimuove manualmente la condivisione dell'indirizzo IP.

Queste funzionalità di rilevamento minacce sono attualmente supportate nelle versioni di Cisco Secure Firewall elencate di seguito:

Software ASA:

- 9.16 versione treno -> supportato dalla 9.16(4)67 e versioni più recenti all'interno di questo treno specifico.
- 9.18 versione treno -> supportato dalla 9.18(4)40 e versioni più recenti all'interno di questo treno specifico.
- 9.20 versione treno -> supportato dalla 9.20(3) e versioni più recenti all'interno di questo treno specifico.
- 9.22 version train -> supportato dalla versione 9.2(1.1) e da tutte le versioni più recenti.

Software FTD:

- 7.0 version train -> supportato dalla versione 7.0.6.3 e dalle versioni più recenti all'interno di questo specifico treno.
- 7.6 version train -> supportato dalla versione 7.6.0 e dalle versioni più recenti.

Nota: queste funzioni non sono attualmente supportate nei treni versione 7.1, 7.2, 7.3 o 7.4. Il documento viene aggiornato non appena diventano disponibili.

Per ulteriori informazioni e per la guida alla configurazione, consultare i seguenti documenti:

- Configurazione su ASA Secure Firewall: configurazione del rilevamento delle minacce per la VPN ad accesso remoto su ASA Secure Firewall.
- Configurazione su FTD Secure Firewall: configurazione del rilevamento delle minacce per i servizi VPN di accesso remoto su Secure Firewall Threat Defense

Opzione 2: applicare misure di protezione avanzata per VPN ad accesso remoto.

Se le funzionalità di rilevamento delle minacce per i servizi VPN ad accesso remoto non sono supportate nella versione del firewall protetto in uso, implementare tutte le misure di protezione avanzata successive per ridurre l'impatto di questi attacchi:

1. Disabilitare l'autenticazione AAA nei profili di connessione DefaultWEBVPN e DefaultRAGroup (procedura dettagliata: ASA) | FTD gestito dal CCP).
2. Disabilitare la postura del firewall sicura (Hostscan) da DefaultWEBVPNGroup e DefaultRAGroup (passaggio per passaggio: ASA) | FTD gestito dal CCP).
3. Disabilitare gli alias di gruppo e abilitare gli URL di gruppo negli altri profili di connessione (procedura dettagliata: ASA) | FTD gestito dal CCP).

Nota: per assistenza con FTD gestito tramite FDM (Firewall Device Management) locale, contattare il Technical Assistance Center (TAC) per ricevere assistenza tecnica.

Per ulteriori informazioni, consultare la guida all'implementazione delle misure di protezione avanzata per la VPN AnyConnect Secure Client.

Opzione 3: Bloccare manualmente i tentativi di connessione da fonti dannose.

Per impedire tentativi di connessione da fonti non autorizzate, è possibile implementare una delle opzioni elencate di seguito:

- Usare il comando "shun":

Questo è un approccio semplice per bloccare un IP dannoso, tuttavia, deve essere fatto manualmente. Per ulteriori informazioni, leggere la sezione Configurazione alternativa per bloccare gli attacchi per un firewall protetto utilizzando il comando 'shun'.

- Configurare l'ACL del control plane:

Implementare un ACL control-plane sull'appliance ASA/FTD per filtrare gli indirizzi IP pubblici non autorizzati e impedire loro di avviare sessioni VPN remote. Configurare i criteri di controllo dell'accesso al Control Plane per la difesa dalle minacce del firewall protetto e l'appliance ASA.

Nota: Cisco Talos ha pubblicato un elenco di indirizzi IP e credenziali associate a questi attacchi. Un collegamento al repository GitHub è disponibile nella sezione "IOC" del relativo advisory. È importante notare che gli indirizzi IP di origine per questo traffico potrebbero cambiare, quindi è necessario esaminare i log di sicurezza (syslog) per identificare gli indirizzi IP problematici. Una volta identificate, le tre opzioni possono essere utilizzate per

---

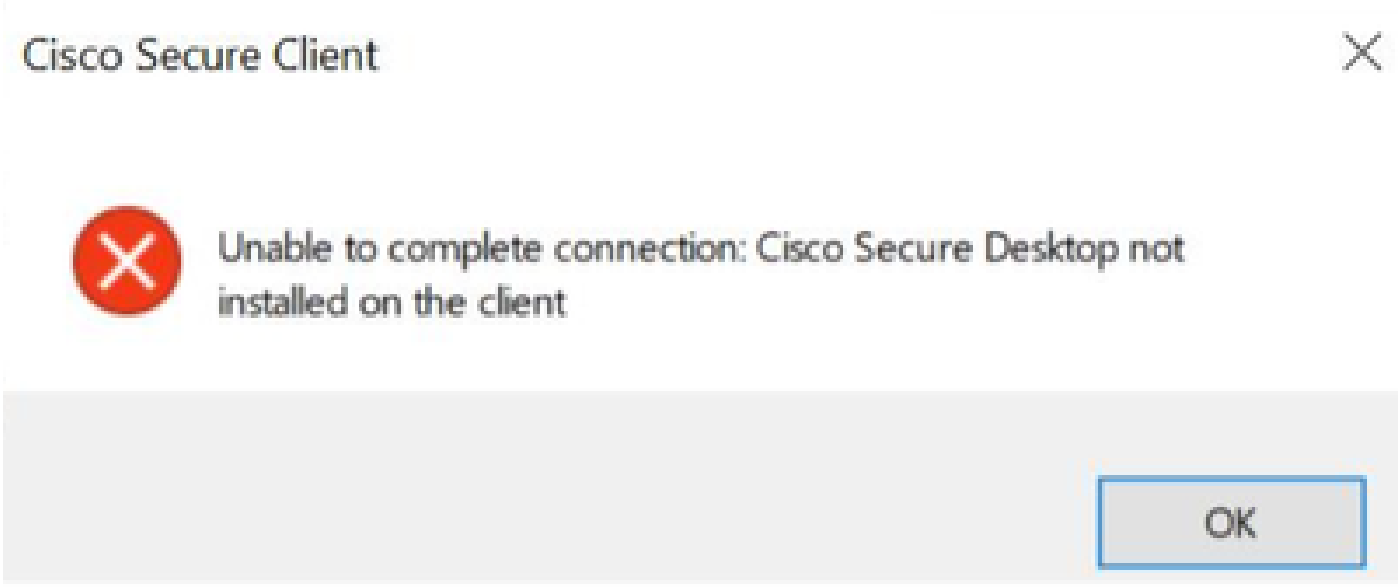
bloccarle.

Comportamenti correlati

Alcuni sintomi possono verificarsi in seguito all'attacco di spray con password da parte del firewall protetto. Per risolvere questi problemi, prendere in considerazione l'implementazione delle raccomandazioni fornite in questo documento.

Sintomo laterale 1: impossibile stabilire connessioni VPN con Cisco Secure Client (AnyConnect) quando la postura del firewall (HostScan) è abilitata

Quando si tenta di stabilire una connessione VPN con Cisco Secure Client (AnyConnect), gli utenti possono ricevere a intermittenza un messaggio di errore del tipo "Impossibile completare la connessione. Cisco Secure Desktop non installato sul client.". Questo comportamento in genere si verifica quando non è possibile allocare un token di scansione host dall'headend VPN, né un'ASA o un FTD Cisco Secure Firewall. In particolare, questo errore di allocazione è correlato a istanze di attacchi di forza bruta destinati all'infrastruttura Secure Firewall e impedisce il completamento corretto del processo di connessione VPN. Questo comportamento è stato rilevato e risolto tramite l'ID bug Cisco CSCwj45822.



Nota: questo comportamento specifico si verifica solo quando all'headend è abilitata la postura del firewall (HostScan), a prescindere dalla versione Secure Client o AnyConnect utilizzata.

Per verificare se l'headend VPN, Cisco Secure Firewall ASA o FTD, mostra i sintomi di errori di allocazione dei token hostscan, eseguire il comando debug menu webvpn 187.0.

<#root>

```
ASA# debug menu webvpn 187 0
Allocated Hostscan token = 1000
```

Hostscan token allocate failure = xxx - - - - > Increments

Nota: il verificarsi di questo problema è una conseguenza degli attacchi. Questo comportamento è stato rilevato e risolto tramite l'ID bug Cisco CSCwj45822.

Per risolvere il problema, valutare la possibilità di implementare le raccomandazioni fornite in questo documento.

Implementazioni di protezione avanzata aggiuntive per RAVPN

È possibile prendere in considerazione ulteriori contromisure che richiedono ulteriori modifiche alle distribuzioni per rafforzare la sicurezza della distribuzione VPN ad accesso remoto, ad esempio l'adozione dell'autenticazione basata su certificati per RAVPN. Per ulteriori informazioni sulla configurazione, consultare il documento sull'implementazione delle misure di protezione avanzata per i client sicuri AnyConnect VPN.

Ulteriori informazioni

- Procedure di indagine forense Cisco ASA per i First Responder
- Procedure di indagine forense di Cisco Firepower Threat Defense per i primi risponditori
- Cisco Talos Threat Advisory
- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.

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).