Wachtwoordspraakaanvallen die gevolgen hebben voor VPN-services van externe toegang

Inhoud

Inleiding

Achtergrondinformatie

Compromisindicatoren (IoC)

- Kan geen VPN-verbindingen maken met Cisco Secure Client (AnyConnect) wanneer Firewallhouding (HostScan) is ingeschakeld
- Ongebruikelijke hoeveelheid verificatieaanvragen

Aanbevelingen

- Vastlegging inschakelen
- Secure Default Remote Access VPN-profielen
- Hefboomwerking TCP-blokkering
- Control-point ACL configureren
- Gebruik op certificaat gebaseerde verificatie voor RAVPN

Inleiding

Dit document beschrijft aanbevelingen om te overwegen tegen aanvallen met wachtwoordspray die zijn gericht op Remote Access VPN (RAVPN)-services die zijn geconfigureerd op Cisco Secure Firewall.

Achtergrondinformatie

Cisco werd op de hoogte gesteld van meerdere rapporten met betrekking tot aanvallen waarbij wachtwoorden worden gesproeid en die op RAVPN-services zijn gericht. Talos heeft opgemerkt dat deze aanvallen niet beperkt zijn tot Cisco-producten, maar ook tot VPN-concentrators van derden.

Afhankelijk van uw omgeving kunnen de aanvallen ertoe leiden dat accounts worden vergrendeld, wat leidt tot DoS-achtige (Denial of Service) omstandigheden.

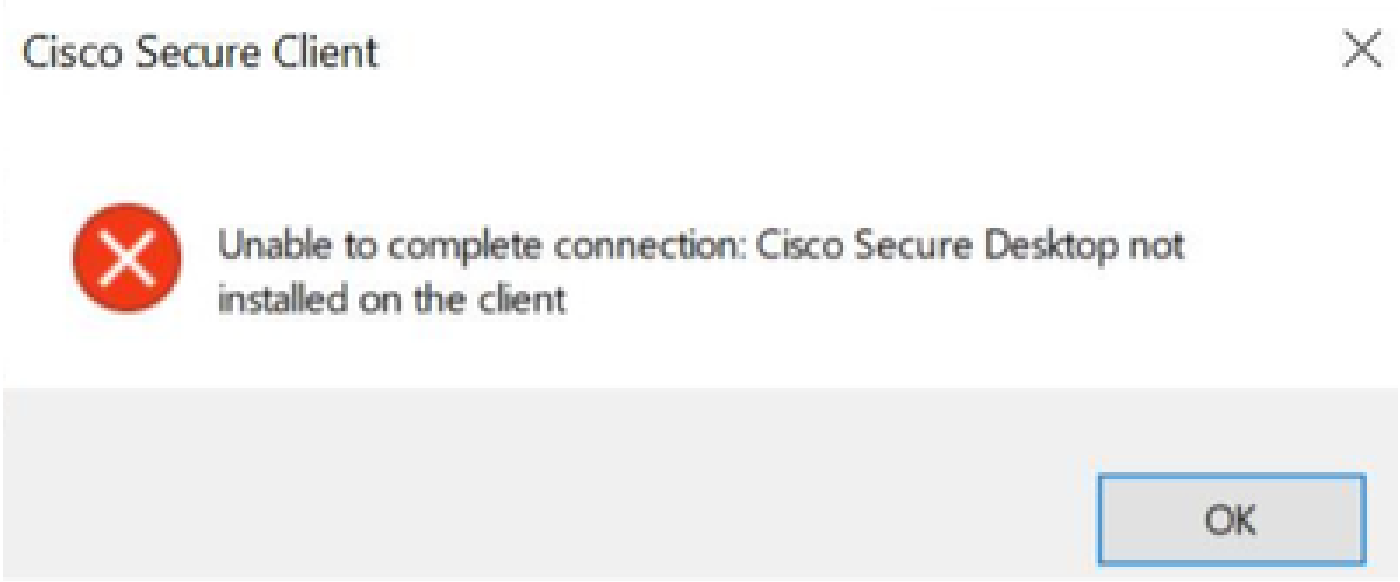
Deze activiteit lijkt verband te houden met verkenningsinspanningen.

Compromisindicatoren (IoC)

Kan geen VPN-verbindingen maken met Cisco Secure Client (AnyConnect) wanneer Firewallhouding (HostScan) is ingeschakeld

Wanneer gebruikers proberen verbinding te maken met Cisco Secure Client (AnyConnect), wordt

hen gevraagd de fout "Kan de verbinding niet voltooien" te ontvangen. Cisco Secure Desktop is niet geïnstalleerd op de client.", waardoor een VPN-verbinding niet met succes kan worden tot stand gebracht.



Dit symptoom lijkt een bijwerking te zijn van de DoS-achtige aanvallen beschreven in het volgende hoofdstuk; verder onderzoek is nog steeds gaande.

Ongebruikelijke hoeveelheid verificatieaanvragen

De VPN head-end Cisco Secure Firewall Adaptive Security Appliance (ASA) of Threat Defence (FTD) vertoont symptomen van aanvallen met wachtwoordspray met 100-duizenden of miljoenen afgewezen verificatiepogingen.

De beste manier om dit te detecteren is door te kijken naar de syslog. Zoek naar een ongebruikelijk aantal van een van de volgende ASA syslog ID's:

- %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-6-113015

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

user

= admin : user

IP

= x.x.x.x

%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-6-113005

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

%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.

%ASA-6-716039

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

```
%ASA-6-716039
: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN.
```

- %ASA-6-725016

De gebruikersnaam is altijd verborgen totdat de opdracht Gebruikersnaam voor niet-vastlegging verbergen op de ASA is geconfigureerd.

Opmerking: dit geeft inzicht om inzicht te hebben als geldige gebruikers worden gegenereerd of bekend door beledigende IP's, maar wees voorzichtig, want gebruikersnamen zullen zichtbaar zijn in de logs.

Om te verifiëren, logt u in op de ASA of FTD Command Line Interface (CLI), voert u de opdracht show aaa-server uit en onderzoekt u of er een ongebruikelijk aantal pogingen en afgewezen verificatieaanvragen is voor een van de geconfigureerde AAA-servers:

<#root>

```
ciscoasa# show aaa-server

Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time 0ms

Number of authentication requests 8473575 - - - - - >>>> Unusual increments


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

Number of rejects 8473574 - - - - - >>>> Unusual increments
```

<#root>

```
ciscoasa# show aaa-server
```

```
Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP 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


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

Aanbevelingen

Het is belangrijk om te benadrukken dat deze aanvallen niet beperkt zijn tot Cisco-producten, maar wereldwijde aanvallen die ook van invloed kunnen zijn op andere leveranciers van derden. De volgende acties zijn aanbevelingen om het effect van deze aanvallen op Cisco Secure Firewall-apparaten tegen te gaan:

Opmerking: ook al zijn deze aanvallen niet specifiek voor CVE-2023-20269, we raden u aan om Secure Firewall software uit te voeren met de oplossing voor deze kwetsbaarheid.

Vastlegging inschakelen

Vastlegging is een cruciaal onderdeel van cyberbeveiliging waarbij gebeurtenissen in een systeem worden vastgelegd. De afwezigheid van gedetailleerde logboeken laat gaten in het begrip, wat een duidelijke analyse van de aanvalsmethode belemmert. Aanbevolen wordt om de logboekregistratie op een externe systeemserver mogelijk te maken voor een betere correlatie en controle van netwerk- en beveiligingsincidenten op verschillende netwerkapparaten.

Zie de volgende platformspecifieke handleidingen voor meer informatie over het configureren van het vastleggen:

Cisco ASA-software:

- Gebruikershandleiding voor Secure ASA Firewall
- Hoofdstuk van logboekregistratie van de configuratiehandleiding voor Cisco Secure Firewall ASA Series General Operations CLI

Cisco FTD-software:

- Logboekregistratie configureren op FTD via FMC
- Syslogsectie configureren in het hoofdstuk Platform-instellingen van de configuratiehandleiding voor apparaten van Cisco Secure Firewall Management Center
- Syslog configureren en controleren in Firepower Device Manager
- Sectie met instellingen voor systeemvastlegging configureren in het hoofdstuk Systeeminstellingen van de Cisco Firepower Threat Defense Configuration Guide voor Firepower Device Manager

Secure Default Remote Access VPN-profielen

Wanneer de standaard externe toegang VPN-verbindingsprofielen/tunnelgroepen DefaultRAGroup en DefaultWEBVPNGroup niet worden gebruikt, is het raadzaam om te voorkomen dat verificatiepogingen en externe toegang VPN-sessieinstelling deze standaardverbindingsprofielen/tunnelgroepen gebruiken door ze naar een AAA-server in de gootsteen te verwijzen. Voer de volgende stappen uit om dit te doen:

1. Configureer een LDAP-server (Light Directory Access Protocol), zoals in het volgende voorbeeld:

```
<#root>
aaa-server
 AAA_Sinkhole
protocol ldap
```

Opmerking: voeg geen extra configuratie toe voor deze AAA-server.

2. Wijs de DefaultRAGgroup,DefaultWEBVPNGgroup, of beide, aan deze dummy LDAP-server, zoals in het volgende voorbeeld:

```
<#root>
```

```
tunnel-group
 DefaultWEBVPNGroup
general-attributes

authentication-server-group
 AAA_Sinkhole

tunnel-group
 DefaultRAGroup
general-attributes

authentication-server-group
 AAA_Sinkhole
```

Hefboomwerking TCP-blokkering

Dit is een eenvoudige benadering om een kwaadaardige IP te blokkeren, maar het moet handmatig worden gedaan. Lees de sectie Alternatieve configuratie om aanvallen voor beveiligde firewall te blokkeren met behulp van de 'shun'-opdracht voor meer informatie.

Control-point ACL configureren

Voer een besturings-vlakke ACL op de ASA/FTD uit om onbevoegde openbare IP-adressen te filteren en te voorkomen dat deze externe VPN-sessies initiëren. Configureer het beleid voor toegangscontrole van besturingsplane voor Secure Firewall Threat Defence en ASA.

Opmerking: voor deze benadering dient u de lijst met IP-adressen die moeten worden geblokkeerd handmatig op te geven en bij te houden.

Gebruik op certificaat gebaseerde verificatie voor RAVPN

Het gebruik van certificaten voor authenticatie biedt een robuustere benadering dan het gebruik van referenties. Om uw omgeving te verharden, kunt u de verificatiemethode voor RAVPN wijzigen om te worden gebaseerd op certificaten.

Controleer voor meer informatie de sectie AAA-instellingen configureren voor externe toegang via VPN in de Cisco Secure Firewall Configuration Guide.

Aanvullende informatie

- Cisco ASA forensische onderzoeksprocedures voor eerste responders
- Cisco-forensische onderzoeksprocedures tegen vuurkracht-bedreigingsverdediging voor eerste transponders

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.