Kennwortsprayangriffe mit Auswirkungen auf Remote Access-VPN-Services

Inhalt

Einleitung

In diesem Dokument werden Empfehlungen für die Abwehr von Passwort-Spray-Angriffen auf RAVPN-Services (Remote Access VPN), die auf der Cisco Secure Firewall konfiguriert sind, beschrieben.

Hintergrundinformationen

Cisco wurde von mehreren Berichten über Angriffe mit Passwortspritzen auf RAVPN-Services in Kenntnis gesetzt. Talos hat festgestellt, dass diese Angriffe nicht nur auf Cisco Produkte beschränkt sind, sondern auch VPN-Konzentratoren von Drittanbietern.

Je nach Umgebung können die Angriffe dazu führen, dass Konten gesperrt werden, was zu Denial of Service (DoS)-ähnlichen Bedingungen führt.

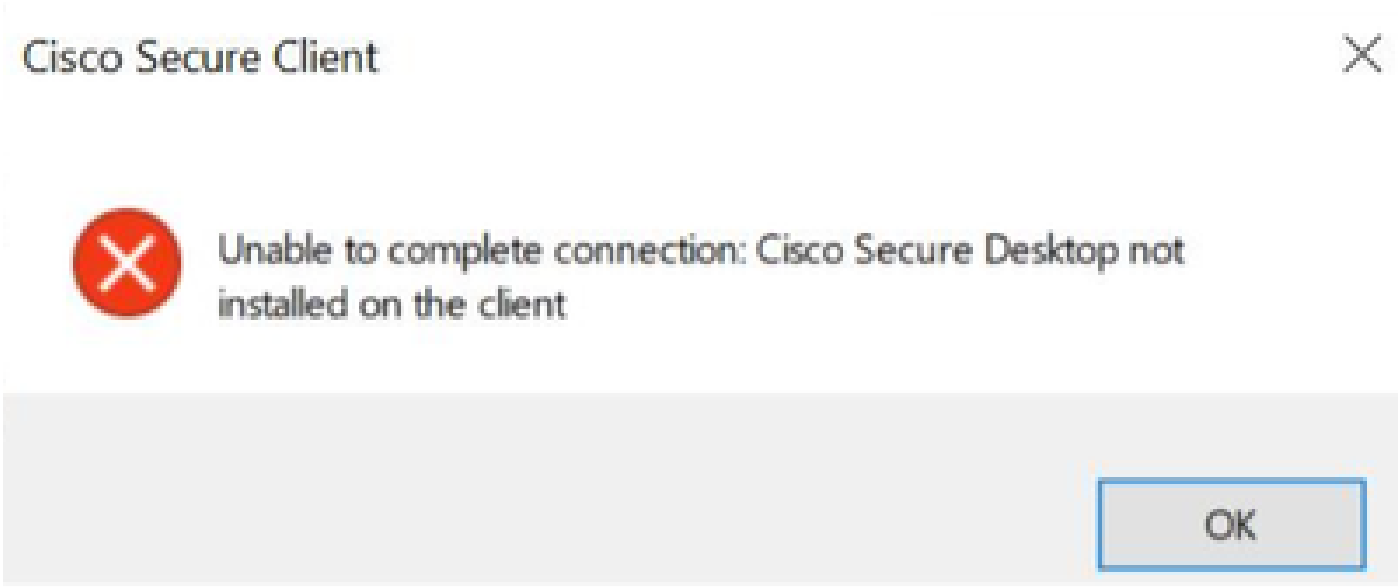
Diese Aktivität scheint mit Aufklärungsbemühungen in Zusammenhang zu stehen.

Indicators of Compromise (IoC)

Bei aktivierter Firewall-Statusüberprüfung (HostScan) können keine VPN-Verbindungen mit dem Cisco Secure Client (AnyConnect) hergestellt werden

Wenn Sie versuchen, eine Verbindung mit dem Cisco Secure Client (AnyConnect) herzustellen, werden die Benutzer aufgefordert, die Fehlermeldung "Verbindung kann nicht hergestellt werden"

zu erhalten. Cisco Secure Desktop nicht auf dem Client installiert.", wodurch die erfolgreiche Herstellung einer VPN-Verbindung verhindert wird.



Dieses Symptom scheint eine Nebenwirkung der im nächsten Abschnitt beschriebenen DoS-ähnlichen Angriffe zu sein; weitere Untersuchungen sind noch im Gange.

Ungewöhnlich viele Authentifizierungsanforderungen

Das VPN-Headend Cisco Secure Firewall Adaptive Security Appliance (ASA) oder Threat Defense (FTD) zeigt Symptome von Passwort-Spray-Angriffen mit 100.000 oder Millionen abgelehnter Authentifizierungsversuche.

Die beste Methode, dies zu erkennen, ist der Blick auf das Syslog. Achten Sie auf eine ungewöhnliche Anzahl der nächsten ASA-Syslog-IDs:

- %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

Der Benutzername wird immer ausgeblendet, bis der Befehl no logging hide username auf der ASA konfiguriert ist.

Hinweis: Dies gibt Aufschluss darüber, ob gültige Benutzer von IP-Adressen generiert oder bekannt sind. Seien Sie jedoch vorsichtig, da die Benutzernamen in den Protokollen angezeigt werden.

Melden Sie sich zur Überprüfung bei der ASA- oder FTD-Befehlszeilenschnittstelle (CLI) an, führen Sie den Befehl show aaa-server aus, und untersuchen Sie die Anzahl der Authentifizierungsanforderungen, die an einen der konfigurierten AAA-Server gesendet werden, wenn Sie eine ungewöhnliche Anzahl von Versuchen und Abweisungen erhalten:

<#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
```

Empfehlungen

Es ist wichtig zu betonen, dass diese Angriffe nicht auf Produkte von Cisco beschränkt sind, sondern auf globale Angriffe, die sich auch auf andere Drittanbieter auswirken können. Die im Folgenden aufgeführten Aktionen dienen als Empfehlungen, wie Sie den Auswirkungen dieser Angriffe auf Cisco Secure Firewall-Geräte begegnen können:

Hinweis: Auch wenn diese Angriffe nicht spezifisch für CVE-2023-20269 sind, empfehlen wir Ihnen, Secure Firewall-Software mit der Behebung dieser Schwachstelle auszuführen.

Protokollierung aktivieren

Protokollierung ist ein wichtiger Bestandteil der Cybersicherheit, bei dem Ereignisse innerhalb eines Systems aufgezeichnet werden. Das Fehlen detaillierter Protokolle hinterlässt Verständnislücken und verhindert eine klare Analyse der Angriffsmethode. Es wird empfohlen, die Protokollierung an einem Remote-Syslog-Server zu aktivieren, um die Korrelation und Überprüfung von Netzwerk- und Sicherheitsvorfällen auf verschiedenen Netzwerkgeräten zu verbessern.

Weitere Informationen zum Konfigurieren der Protokollierung finden Sie in den folgenden plattformspezifischen Leitfäden:

Cisco ASA Software:

- Benutzerhandbuch für sichere ASA-Firewall
- ProtokollKapitel des Konfigurationsleitfadens für die allgemeine Betriebs-CLI der Cisco Secure Firewall ASA-Serie

Cisco FTD-Software:

- Konfigurieren der Protokollierung auf FTD über FMC
- Konfigurieren Sie Syslog im Kapitel "Plattform-Einstellungen" des Cisco Secure Firewall Management Center Gerätekonfigurationsleitfadens.
- Konfiguration und Überprüfung des Syslog im FirePOWER Geräte-Manager
- Abschnitt "Einstellungen der Systemprotokollierung" im Kapitel "Systemeinstellungen" des Cisco Firepower Threat Defense-Konfigurationsleitfadens für den Firepower-Gerätemanager konfigurieren

Sichere Standard-VPN-Profile für den Remote-Zugriff

Wenn die standardmäßigen VPN-Verbindungsprofile/Tunnelgruppen für den Remotezugriff DefaultRAGroup und DefaultWEBVPNGroup nicht verwendet werden, wird empfohlen, Authentifizierungsversuche und den Aufbau von VPN-Sitzungen für den Remotezugriff mithilfe dieser standardmäßigen Verbindungsprofile/Tunnelgruppen zu verhindern, indem sie auf einen AAA-Server für das Systemabsturz verweisen. Gehen Sie dazu wie folgt vor:

1. Konfigurieren Sie einen Dummy-LDAP-Server (Lightweight Directory Access Protocol), wie im folgenden Beispiel gezeigt:

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

Hinweis: Fügen Sie keine zusätzliche Konfiguration für diesen AAA-Server hinzu.

2. Zeigen Sie auf DefaultRAGroup, DefaultWEBVPNGroup oder beide auf diesen Dummy-LDAP-Server, wie im nächsten Beispiel gezeigt:

<#root>

tunnel-group

DefaultWEBVPNGroup

general-attributes

authentication-server-group

AAA_Sinkhole

tunnel-group

DefaultRAGroup

general-attributes

authentication-server-group

AAA_Sinkhole

TCP-Shun nutzen

Dies ist ein unkomplizierter Ansatz zum Blockieren einer schädlichen IP-Adresse. Er muss jedoch manuell durchgeführt werden. Weitere Informationen finden Sie im Abschnitt Alternative Konfiguration zum Blockieren von Angriffen für sichere Firewalls mit dem Befehl "shun".

Konfigurieren der Control Plance ACL

Implementieren Sie eine ACL auf Kontrollebene auf der ASA/FTD, um nicht autorisierte öffentliche IP-Adressen herauszufiltern und zu verhindern, dass diese Remote-VPN-Sitzungen initiieren. Konfigurieren Sie Zugriffskontrollrichtlinien für die Kontrollebene für die sichere Abwehr von Firewall-Bedrohungen und ASA.

Hinweis: Bei diesem Ansatz müssen Sie die Liste der zu sperrenden IP-Adressen manuell festlegen und verwalten.

Zertifikatbasierte Authentifizierung für RAVPN verwenden

Die Verwendung von Zertifikaten für die Authentifizierung stellt im Vergleich zur Verwendung von Anmeldeinformationen einen robusteren Ansatz dar. Um Ihre Umgebung zu schützen, können Sie

die Authentifizierungsmethode für RAVPN so ändern, dass sie auf Zertifikaten basiert.

Weitere Informationen finden Sie im Abschnitt Konfigurieren der AAA-Einstellungen für Remote Access VPN im Cisco Secure Firewall Configuration Guide.

Zusätzliche Informationen

- Cisco ASA Forensische Untersuchungsverfahren für Einsatzkräfte
- Cisco FirePOWER Threat Defense - Forensische Ermittlungsverfahren für Einsatzkräfte

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.