원격 액세스 VPN 서비스에 영향을 미치는 비밀번호 스프레이 공격

목차

[소개](#)

[배경 정보](#)

[보안 침해 지표(IoC)](#)

- [Firewall Posture(HostScan)가 활성화된 경우 Cisco Secure Client(AnyConnect)와의 VPN 연결을 설정할 수 없음](#)
- [비정상적인 양의 인증 요청](#)

[권장 사항](#)

- [로깅 사용](#)
- [보안 기본 원격 액세스 VPN 프로파일](#)
- [TCP 차단 활용](#)
- [Control-plus ACL 구성](#)
- [RAVPN에 인증서 기반 인증 사용](#)

소개

이 문서에서는 Cisco Secure Firewall에 구성된 RAVPN(Remote Access VPN) 서비스를 대상으로 하는 비밀번호 스프레이 공격을 방지하기 위해 고려해야 할 권장 사항에 대해 설명합니다.

배경 정보

Cisco는 RAVPN 서비스를 겨냥한 비밀번호 살포 공격과 관련된 여러 보고서를 알고 있었습니다. Talos는 이러한 공격이 Cisco 제품뿐만 아니라 서드파티 VPN Concentrator에 국한되지 않는다고 지적했습니다.

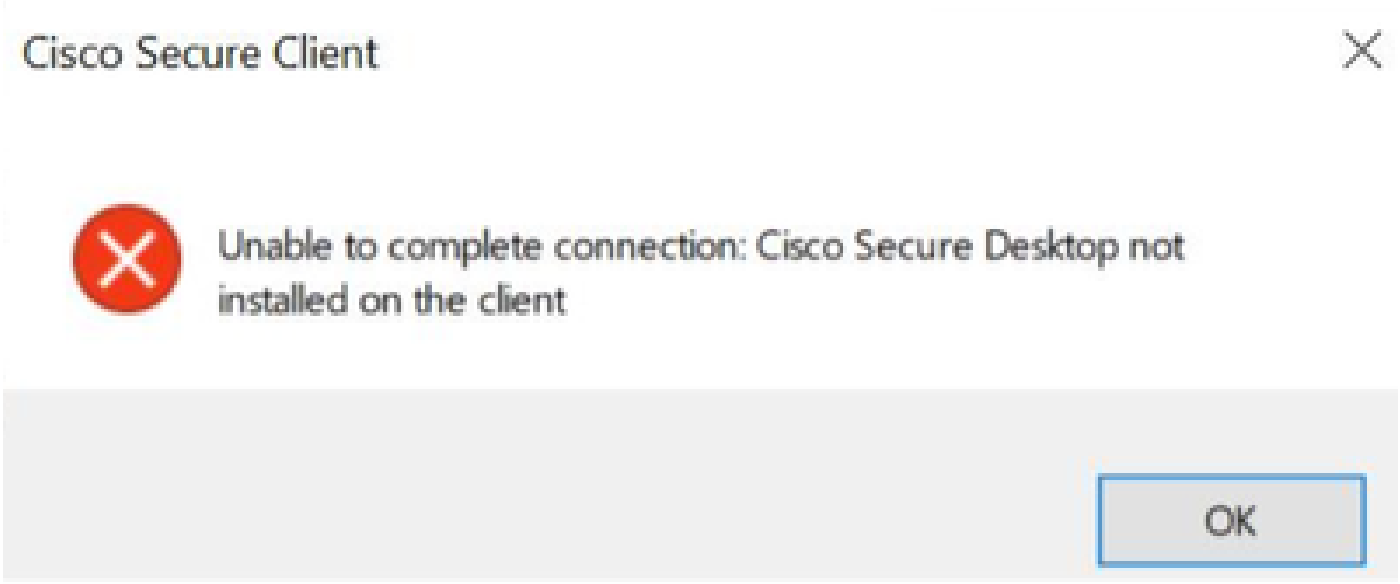
사용자 환경에 따라, 공격으로 인해 계정이 잠기면서 DoS(Denial of Service) 유사 상태가 발생할 수 있습니다.

이 활동은 정찰 노력과 관련이 있는 것으로 보인다.

보안 침해 지표(IoC)

Firewall Posture(HostScan)가 활성화된 경우 Cisco Secure Client(AnyConnect)와의 VPN 연결을 설정할 수 없음

Cisco Secure Client(AnyConnect)에 연결하려고 하면 사용자에게 "연결을 완료할 수 없습니다. Cisco Secure Desktop이 클라이언트에 설치되지 않았습니다.", VPN 연결을 성공적으로 설정하지 못했습니다.



이 증상은 다음 섹션에서 설명하는 DoS 유사 공격의 부작용으로 보이며, 추가 조사는 아직 진행 중입니다.

비정상적인 양의 인증 요청

VPN 헤드엔드 Cisco ASA(Secure Firewall Adaptive Security Appliance) 또는 FTD(Threat Defense)는 비밀번호 스프레이 공격의 증상을 보여주며, 인증 시도는 10만 또는 수백만 건이 거부됩니다.

이를 탐지하는 가장 좋은 방법은 syslog를 확인하는 것입니다. 다음 ASA syslog ID 중 특이한 숫자를 찾습니다.

- %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

사용자 이름은 ASA에서 no logging hide username 명령이 구성될 때까지 항상 숨겨집니다.

참고: 이렇게 하면 잘못된 IP를 통해 유효한 사용자가 생성되었거나 알려진 것인지 파악할 수 있습니다. 그러나 사용자 이름이 로그에 표시되므로 주의하십시오.

확인하려면 ASA 또는 FTD CLI(Command Line Interface)에 로그인하고 show aaa-server 명령을 실행하고 구성된 AAA 서버 중 하나에 대해 시도하거나 거부된 비정상적인 인증 요청 횟수를 조사합니다.

<#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
```

권장 사항

이러한 공격은 Cisco 제품에만 국한되지 않고 다른 서드파티 벤더에도 영향을 미칠 수 있는 글로벌 공격이라는 점을 강조해야 합니다. 다음은 Cisco Secure Firewall 디바이스를 대상으로 하는 이러한 공격의 영향에 대응하기 위한 권장 조치입니다.

참고: 이러한 공격은 CVE-2023-20269에 국한되지 않지만, 이 취약성에 대한 수정 사항과 함께 Secure Firewall 소프트웨어를 실행하는 것이 좋습니다.

로깅 사용

로깅은 시스템 내에서 발생하는 이벤트를 기록하는 것과 관련된 사이버 보안의 중요한 부분입니다. 세부 로그가 없으면 이해의 공백이 생겨 공격 방법에 대한 명확한 분석이 방해된다. 다양한 네트워크 디바이스에서 네트워크 및 보안 인시던트의 상관관계 및 감사를 개선하려면 원격 syslog 서버에 대한 로깅을 활성화하는 것이 좋습니다.

로깅을 구성하는 방법에 대한 자세한 내용은 다음 플랫폼별 가이드를 참조하십시오.

Cisco ASA 소프트웨어:

- 보안 ASA 방화벽 사용 설명서
- Cisco Secure Firewall ASA Series 일반 작업 CLI 컨피그레이션 가이드의 로그인 장

Cisco FTD 소프트웨어:

- FMC를 통해 FTD에 로깅 구성
- Cisco Secure Firewall Management Center Device Configuration Guide의 Platform Settings

장에서 Syslogsection을 구성합니다
- firepower 장치 관리자에서 Syslog 구성 및 확인
- Firepower 디바이스 관리자용 Cisco Firepower Threat Defense 컨피그레이션 가이드의 시스템 설정 장에서 시스템 로깅 설정 구성 섹션

보안 기본 원격 액세스 VPN 프로파일

기본 원격 액세스 VPN 연결 프로파일/터널 그룹 DefaultRAGroup 및 DefaultWEBVPNGroup을 사용하지 않는 경우 싱크홀 AAA 서버를 가리키도록 하여 이러한 기본 연결 프로파일/터널 그룹을 사용한 인증 시도 및 원격 액세스 VPN 세션 설정을 방지하는 것이 좋습니다. 이렇게 하려면 다음 단계를 수행하십시오.

1. 다음 예와 같이 더미 LDAP(Lightweight Directory Access Protocol) 서버를 구성합니다.

```
<#root>

aaa-server

 AAA_Sinkhole

protocol ldap
```

참고: 이 AAA 서버에 대한 추가 컨피그레이션을 추가하지 마십시오.

2. 다음 예에 표시된 것처럼 DefaultRAGroup,DefaultWEBVPNGroup 또는 둘 모두를 이 더미 LDAP 서버로 가리킵니다.

```
<#root>

tunnel-group

 DefaultWEBVPNGroup

general-attributes


authentication-server-group

 AAA_Sinkhole


tunnel-group

 DefaultRAGroup
```

```
general-attributes


authentication-server-group
 AAA_Sinkhole
```

TCP 차단 활용

이는 악의적인 IP를 차단하기 위한 간단한 접근 방식이지만 수동으로 수행해야 합니다. 자세한 내용은 'shun' 명령을 사용하여 보안 방화벽의 공격을 차단하는 대체 컨피그레이션 섹션을 참조하십시오.

Control-plus ACL 구성

ASA/FTD에서 컨트롤 플레인 ACL을 구현하여 무단 공용 IP 주소를 필터링하고 이들이 원격 VPN 세션을 시작하지 못하도록 합니다. 보안 방화벽 위협 방어 및 ASA에 대한 컨트롤 플레인 액세스 제어 정책을 구성합니다.

참고: 이 접근 방식에서는 차단할 IP 주소 목록을 수동으로 지정하고 유지 관리해야 합니다.

RAVPN에 인증서 기반 인증 사용

인증을 위한 인증서 사용은 자격 증명 사용에 비해 더 강력한 접근 방식을 제공합니다. 환경을 강화하려면 인증서를 기반으로 하는 RAVPN의 인증 방법을 변경할 수 있습니다.

자세한 내용은 Cisco Secure Firewall Configuration Guide의 Configure AAA Settings for Remote Access VPN 섹션을 참조하십시오.

추가 정보

- 첫 번째 대응자를 위한 Cisco ASA 포렌식 조사 절차
- Cisco Firepower Threat Defense 포렌식 조사 절차(최초 대응자)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.