リモートアクセスVPNサービスに影響を与えるパスワードスプレー攻撃

内容

はじめに

このドキュメントでは、Cisco Secure Firewallに設定されたリモートアクセスVPN(RAVPN)サービスを対象としたパスワードスプレー攻撃に対して考慮すべき推奨事項について説明します。

背景説明

シスコは、RAVPNサービスを対象としたパスワードスプレー攻撃に関連する複数のレポートを認識しました。Talosは、これらの攻撃がシスコ製品だけでなくサードパーティのVPNコンセントレータにも限定されないことを指摘しています。

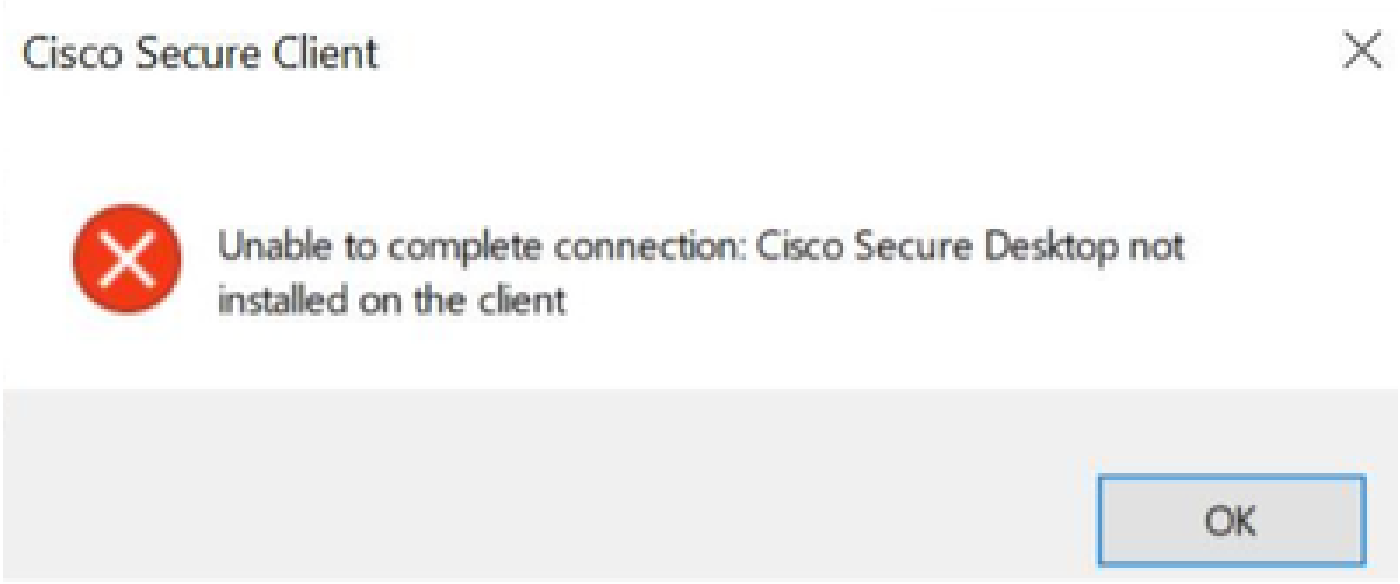
環境によっては、攻撃によってアカウントがロックされ、サービス拒否(DoS)のような状態になる可能性があります。

この活動は偵察活動に関連しているようです。

セキュリティ侵害の指標(IoC)

ファイアウォールポスチャ(HostScan)が有効な場合に、Cisco Secure Client(AnyConnect)とのVPN接続を確立できない

Cisco Secure Client(AnyConnect)に接続しようとすると、エラー「Unable to complete connection.Cisco Secure Desktop not installed on the client.」というエラーメッセージが表示され、VPN接続の確立が失敗します。



この症状は、次のセクションで説明するDoSに似た攻撃の副作用と考えられます。詳細な調査は現在も進行中です。

通常とは異なる量の認証要求

VPNヘッドエンドのCisco Secure Firewall Adaptive Security Appliance(ASA)またはThreat Defense(FTD)では、10万回または数百万の認証試行の拒否によるパスワードスプレー攻撃の症状が示されます。

これを検出する最善の方法は、syslogを調べることです。次のASA syslog IDの中で異常な数を探します。

- %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

ユーザ名は、ASAでno logging hide usernameコマンドが設定されるまで、常に非表示になります。

注：これにより、有効なユーザが生成されたか、または問題のIPによって既知であるかを理解するための情報が得られます。ただし、ユーザ名はログに表示されるため、注意が必要です。

確認するには、ASAまたはFTDのコマンドラインインターフェイス(CLI)にログインし、show aaa-serverコマンドを実行して、設定されたAAAサーバのいずれかに対して試行された認証要求と拒否された認証要求の数が異常でないかどうかを調べます。

<#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
```

推奨事項

これらの攻撃はシスコ製品に限定されず、他のサードパーティベンダーにも影響を与える可能性のあるグローバルな攻撃であることを強調することが重要です。次に示すアクションは、Cisco Secure Firewallデバイスに対するこれらの攻撃の影響に対処するための推奨事項です。

注：これらの攻撃がCVE-2023-20269に固有のものではない場合でも、この脆弱性の修正を含むセキュアファイアウォールソフトウェアを実行することをお勧めします。

Enable Logging

ロギングは、システム内で発生するイベントを記録するサイバーセキュリティの重要な部分です。詳細なログが存在しないため、理解にギャップが生じ、攻撃方法の明確な分析に支障をきたします。リモートsyslogサーバへのロギングを有効にして、さまざまなネットワークデバイス間のネットワークおよびセキュリティインシデントの関連付けと監査を改善することを推奨します。

ロギングの設定方法については、次のプラットフォーム固有のガイドを参照してください。

Cisco ASAソフトウェア：

- ガイドを使用したASAファイアウォールの保護
- 『Cisco Secure Firewall ASAシリーズ一般動作CLIコンフィギュレーションガイド』の「ロギング」の章

Cisco FTDソフトウェア：

- FMC を介して FTD にロギングを設定
- 『Cisco Secure Firewall Management Center Device Configuration Guide』の「Platform Settings」の章の「Configure Syslogsection」
- Firepower Device Manager(FDM)でのsyslogの設定と確認
- 『Cisco Firepower Threat Defense Firepower Device Manager用コンフィギュレーションガイド』の「システム設定」の章の「システムロギング設定の設定」の項

デフォルトのリモートアクセスVPNプロファイルの保護

デフォルトのリモートアクセスVPN接続プロファイル/トンネルグループDefaultRAGroupおよびDefaultWEBVPNGroupを使用しない場合は、これらのデフォルト接続プロファイル/トンネルグループをシンクホールAAAサーバに指定することによって、認証の試行と、これらのデフォルト接続プロファイル/トンネルグループを使用したリモートアクセスVPNセッションの確立を防止することをお勧めします。これを行うには、次の手順に従います。

1.次の例に示すように、ダミーのLightweight Directory Access Protocol(LDAP)サーバを設定します。

```
<#root>

aaa-server

 AAA_Sinkhole

protocol ldap
```

注：このAAAサーバの設定を追加しないでください。

2.次の例に示すように、DefaultRAGroup、DefaultWEBVPNGroup、またはその両方をこのダミーLDAPサーバにポイントします。

```
<#root>

tunnel-group

 DefaultWEBVPNGroup

general-attributes


authentication-server-group

 AAA_Sinkhole
```

```
tunnel-group
 DefaultRAGroup
general-attributes

authentication-server-group
 AAA_Sinkhole
```

TCP回避の活用

これは悪意のあるIPをブロックする簡単なアプローチですが、手動で行う必要があります。詳細については、「shunコマンドを使用してセキュアファイアウォールの攻撃をブロックする代替設定」を参照してください。

コントロールプレーンACLの設定

ASA/FTDにコントロールプレーンACLを実装して、不正なパブリックIPアドレスをフィルタリングし、リモートVPNセッションの開始を防止します。 セキュアファイアウォール脅威対策およびASA用のコントロールプレーンアクセスコントロールポリシーを設定します。

注：この方法では、ブロックするIPアドレスのリストを手動で指定し、維持する必要があります。

RAVPNに証明書ベースの認証を使用する

認証に証明書を使用すると、クレデンシャルを使用するよりも堅牢なアプローチが提供されます。環境を強化するために、RAVPNの認証方式を証明書に基づくように変更できます。

詳細については、『Cisco Secure Firewallコンフィギュレーションガイド』の「リモートアクセスVPNのAAA設定の設定」セクションを参照してください。

追加情報

- Cisco ASAの第一応答者に対するフォレンジック調査手順

- 第一応答者用のCisco Firepower Threat Defenseフォレンジック調査手順

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。