针对影响远程访问VPN服务的密码喷雾攻击的最佳实践

目录

简介

本文档介绍针对针对在思科安全防火墙上配置的远程访问VPN(RAVPN)服务的密码喷雾攻击所考虑的建议。

背景信息

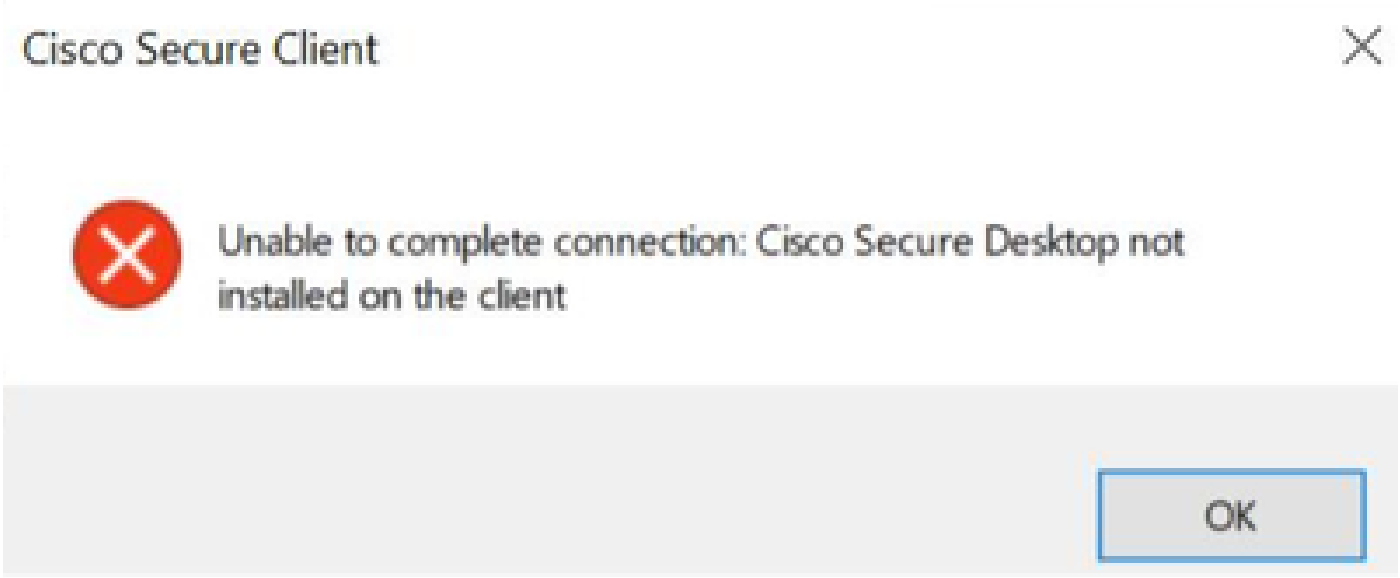
思科获知了多个与针对RAVPN服务的密码攻击相关的报告。Talos指出，这些攻击不仅限于思科产品，还包括第三方VPN集中器。

此活动似乎与侦察工作有关。

观察到的异常模式

启用防火墙状态(HostScan)时，无法与Cisco安全客户端(AnyConnect)建立VPN连接

尝试连接Cisco Secure Client(AnyConnect)时，用户会收到提示，提示其收到错误“Unable to complete connection（无法完成连接）”。客户端上未安装Cisco Secure Desktop。"导致无法成功建立VPN连接。



此症状似乎为下一节描述的类似DoS攻击的副作用；进一步的内部调查仍在进行中。

注意：仅在头端配置了防火墙状态(HostScan)的情况下观察到此特定行为。

异常数量的身份验证请求

VPN头端思科安全防火墙自适应安全设备(ASA)或威胁防御(FTD)显示密码喷雾攻击的症状，身份验证尝试被拒绝次数高达10万次或数百万次。

检测此情况的最佳方法是查看系统日志。查找任何下一个ASA系统日志ID的异常数量：

- %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.

在ASA上配置no logging hide username命令之前，用户名始终处于隐藏状态。

注意：这将有助于了解是否通过违规IP生成或认识了有效用户，但请注意用户名在日志中可见。

要验证，请登录到ASA或FTD命令行界面(CLI)，运行show aaa-server命令，并调查尝试和拒绝的到任何已配置AAA服务器的身份验证请求的不寻常数量：

<#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
```

建议

下面列出的操作是针对思科安全防火墙设备的建议来对抗这些攻击的影响：

1.启用日志记录

日志记录是网络安全的重要组成部分，涉及记录系统中发生的事件。由于没有详细的日志，在理解方面仍存在差距，妨碍了对攻击方法的清晰分析。建议您启用远程系统日志服务器的日志记录，以改进跨各种网络设备的网络和安全事件的关联和审核。

有关如何配置日志记录的信息，请参阅以下特定于平台的指南：

Cisco ASA软件：

- 使用指南保护ASA防火墙
- Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide中的日志记录一章

思科FTD软件：

- 通过 FMC 在 FTD 上配置日志记录
- Cisco Secure Firewall Management Center Device Configuration Guide的Platform Settings一章中的Configure Syslog部分
- 在Firepower设备管理器中配置和验证系统日志
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager的System Settings一章中的Configuring System Logging Settings部分

2.安全默认远程访问VPN配置文件

当不使用默认远程访问VPN连接配置文件/隧道组DefaultRAGroup和DefaultWEBVPNGroup时，建议使用这些默认连接配置文件/隧道组，通过将身份验证尝试和远程访问VPN会话建立指向Sinkhole AAA服务器。为此，请执行以下步骤：

1.配置一个虚拟轻量级目录访问协议(LDAP)服务器，如下例所示：

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

注意：请勿为此AAA服务器添加任何其他配置。

2.将DefaultRAGroup 和DefaultWEBVPNGroup 指向此虚拟LDAP服务器，如下例所示：

```
<#root>
tunnel-group
 DefaultWEBVPNGroup
```

```
general-attributes

authentication-server-group
 AAA_Sinkhole

tunnel-group
 DefaultRAGroup
general-attributes

authentication-server-group
 AAA_Sinkhole
```

注意：如果在默认组重定向到AAA_Sinkhole服务器后，攻击者以合法连接配置文件（隧道组）为目标，则必须阻止这些连接尝试。有关详细信息，请参阅后续部分。

3.阻止来自恶意源的连接尝试

为了阻止来自未授权源的连接尝试，您可以实施下列任一选项：

注意：最初，您必须查看安全日志(syslog)以确定有问题的IP地址。识别后，可以使用这3个选项中的任意一个来阻止它们。

注意：您必须手动指定并维护要阻止的IP地址列表。

实施接口级ACL

在ASA/FTD上实施接口级ACL以过滤未授权的公有IP地址并防止它们启动远程VPN会话。

使用“shun”命令

这是一种直接的阻止恶意IP的方法，但必须手动完成。有关详细信息，请阅读使用“shun”命令阻止安全防火墙攻击的备用配置部分。

配置控制范围ACL

在ASA/FTD上实施控制平面ACL以过滤未授权的公有IP地址并防止它们启动远程VPN会话。 为安全防火墙威胁防御和ASA配置控制平面访问控制策略。

对RAVPN使用基于证书的身份验证（可选）

与使用凭证相比，使用证书进行身份验证可提供更稳健的方法。要加固环境，可以将RAVPN的身份验证方法更改为基于证书。

有关详细信息，请查看《Cisco安全防火墙配置指南》中的配置远程访问VPN的AAA设置部分。

其他信息

- 适用于第一响应者的Cisco ASA调查调查程序
- 面向第一响应者的思科Firepower威胁防御调查程序

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。