缓解远程VPN安全防火墙上的密码喷雾攻击

目录

简介

背景信息

观察到的行为

- 被拒绝的身份验证请求数量异常

建议

- 1.启用日志记录
- 2.配置远程访问VPN的威胁检测功能或强化措施
  - 选项1（推荐）：为远程访问VPN服务配置威胁检测
  - 选项 2：对远程访问VPN应用强化措施

相关行为

- Cisco Bug ID CSCwj45822（仅限注册用户）：Cisco ASA和FTD软件远程访问VPN暴力拒绝服务漏洞(CVE-2024-20481)

Additional Information

简介

本文档介绍针对针对安全防火墙中远程访问VPN服务的密码喷雾攻击所考虑的建议。

背景信息

密码喷雾攻击是一种暴力攻击，攻击者在多个帐户中系统地使用几个常用的密码，尝试对多个用户帐户进行未经授权的访问。成功的密码喷雾攻击可能导致对敏感信息的未经授权的访问、数据泄露以及网络完整性受到潜在威胁

此外，即使这些攻击尝试访问失败，它们也会消耗来自安全防火墙的计算资源，并阻止有效用户连接到远程访问VPN服务。

观察到的行为

当您的安全防火墙成为远程访问VPN服务中的密码喷雾攻击的目标时，您可以通过监控系统日志和运行特定的show命令来识别这些攻击。要查找的最常见行为包括：

被拒绝的身份验证请求数量异常

VPN头端Cisco安全防火墙ASA或FTD显示密码喷雾攻击的症状，以及不寻常的拒绝身份验证尝试率。

> 注意：这些不寻常的身份验证尝试可定向到LOCAL数据库或外部身份验证服务器。

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：这样可以验证是否生成了有效的用户，或者是否通过违规的IP获知有效的用户。但是，请谨慎使用，因为用户名在日志中可见。

要进行验证，请登录ASA或FTD命令行界面(CLI)并运行show aaa-server命令。检查向任何已配置的AAA服务器发出的尝试和拒绝的身份验证请求的不寻常数量：

<#root>

```
ciscoasa# show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against external 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 / Unusual rejection rate


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

考虑并应用下述建议：

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，在了解攻击方法方面存在差距，并妨碍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：

- 安全ASA防火墙指南
- 思科安全防火墙ASA系列常规操作CLI配置CLI日志记录指南

思科FTD软件：

- 通过防火墙管理中心(FMC)配置FTD登录
- Cisco Secure Firewall Management Center Device Configuration Guide的Platform Settings一章中的Configure Syslog部分
- 在 Firepower Device Manager 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

注意：系统日志消息ID对于验证本文档中概述的行为(113015、113005和716039)是必需的。必须在信息级别(6)启用它们，因为这些ID属于“auth”和“webvpn”日志记录类。

2.配置远程访问VPN的威胁检测功能或强化措施

为了帮助减轻这些暴力攻击对RAVPN连接的影响并降低发生这种攻击的可能性，您可以查看并应用以下配置选项：

选项1（推荐）：为远程访问VPN服务配置威胁检测

针对远程访问VPN服务的威胁检测功能通过自动阻止超过配置阈值的主机（IP地址）来阻止来自IPv4地址的DoS（拒绝服务）攻击，从而阻止进一步的尝试，直到您手动删除IP地址的回避。有单独的服务可用于以下类型的攻击：

- 对远程访问VPN服务的身份验证尝试反复失败（暴力用户名/密码扫描攻击）。
- 客户端发起攻击，攻击者从单个主机发起攻击但不完成从远程访问VPN头端重复的连接尝试。
- 当攻击者尝试连接到仅用于设备内部功能的特定内置隧道组时，连接会尝试无效的远程访问VPN服务。合法终端不得尝试连接到这些隧道组。

以下列出的思科安全防火墙版本当前支持这些威胁检测功能：

ASA软件：

- 9.16版本系列->从9.16(4)67及此特定系列中的更新版本支持。
- 9.17版本系列->支持9.17(1)45及此特定系列中的更新版本。
- 9.18版本系列->支持9.18(4)40及此特定系列中的更新版本。
- 9.19版本系列->从9.19(1)。37及此特定系列中的更新版本支持。
- 9.20版本系列->支持9.20(3)和此特定系列中的更新版本。
- 9.22版本系列->从9.22(1.1)及任何更新版本支持。

FTD软件：

- 7.0版本系列->支持7.0.6.3及此特定系列中的更新版本。
- 7.2版本系列->支持7.2.9及此特定系列中的更新版本。

- 7.4版本系列->支持7.4.2.1及此特定系列中的更新版本。
- 7.6版本系列->从7.6.0及任何更新版本中受支持。

注意：这些功能目前在版本7.1或7.3系列中不受支持。

有关完整的详细信息和配置帮助，请参阅文档指南：

- 在安全防火墙ASA上的配置：为安全防火墙ASA上的远程访问VPN配置威胁检测
- 在FMC管理的安全防火墙FTD上配置：在安全防火墙管理中心上配置远程访问VPN服务的威胁检测
- FDM管理的安全防火墙FTD上的配置：在安全防火墙设备管理器上配置远程访问VPN服务的威胁检测

选项 2：对远程访问VPN应用强化措施

注意：这些措施只能帮助降低风险，但是它们不是针对针对RAVPN服务的DoS攻击的预防措施。

如果您的安全防火墙版本不支持远程访问VPN服务的威胁检测功能，请实施加强措施来降低这些攻击带来的风险：

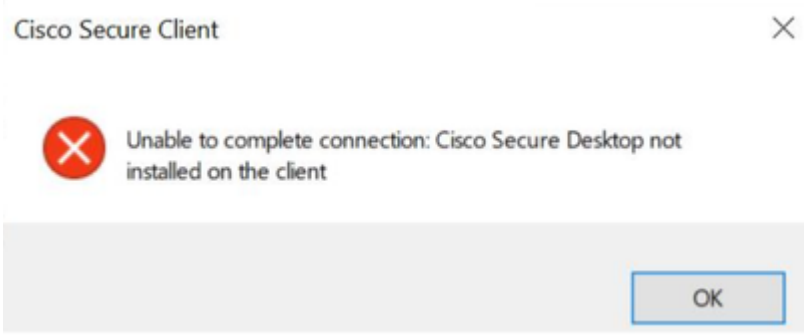
1. 在DefaultWEBVPN和DefaultRAGroup连接配置文件中禁用AAA身份验证(分步：ASA|FTD Managed by FMC)。
2. 从DefaultWEBVPNGroup和DefaultRAGroup禁用安全防火墙状态(Hostscan)(分步：ASA|FTD Managed by FMC)。
3. 在连接配置文件的其余部分中禁用组别名和启用组URL(分步：ASA|FTD Managed by FMC)。

注意：如果您需要通过本地防火墙设备管理(FDM)管理的FTD需要其他支持，请联系Cisco TAC获取专家指导。

有关详细信息，请参阅实施安全客户端AnyConnect VPN的加固措施指南。

相关行为

当安全防火墙上启用防火墙状态(HostScan)时，用户可能会遇到无法与思科安全客户端(AnyConnect)建立VPN连接的情况。它可能会间歇性地遇到错误消息“Unable to complete connection(无法完成连接)”。客户端上未安装Cisco Secure Desktop。"



此行为是成功利用漏洞CVE-2024-20481的结果，下文将对此进行描述。

思科漏洞ID CSCwj45822: Cisco ASA和FTD软件远程访问VPN暴力拒绝服务漏洞(CVE-2024-20481)

此漏洞源于密码喷雾攻击造成的资源耗尽，攻击者向目标设备发送大量VPN身份验证请求。成功利用此漏洞可导致RAVPN服务的拒绝服务。此漏洞的一个主要症状是用户间歇性地遇到“Unable to complete connection(无法完成连接)”。客户端上未安装Cisco Secure Desktop。" 当它们尝试使用Cisco安全客户端建立RAVPN连接时显示错误消息。

要解决此漏洞，必须升级到安全建议中列出的软件版本。此外，建议您在安全防火墙升级到这些版本后启用远程访问VPN的威胁检测功能，以防御针对RAVPN服务的DoS攻击。

有关完整详细信息，请参阅Cisco ASA和FTD软件远程访问VPN暴力拒绝服务漏洞安全建议。

Additional Information

- 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
- Cisco Talos威胁建议

如需其他帮助，请联系思科TAC。需要有效的支持合同： 思科全球支持联系方式.

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）。