

使用本地链路AAA服务器地址的安全访问RA VPN身份验证事件

目录

问题

测试安全访问远程访问(RA)VPN功能时，会为租户组织中不存在的标识记录过多的身份验证事件。身份验证日志显示24小时内超过10,000个RA VPN身份验证事件，其中包含AAA错误，例如“AAALOG_SERVICE_DOWN”和“AAALOG_SERVER_DOWN”。这些错误消息引用本地链路169.254.x.x地址作为AAA服务器，这些地址未在租户中配置。

日志中观察到的具体错误示例包括：

AAALOG_SERVICE_DOWN

AAA authentication server not accessible : server = 169.254.169.79 : user = <user>

AAALOG_SERVER_DOWN

AAA Marking RADIUS server 169.254.169.79 as FAILED

本练习似乎重复了针对安全访问VPN FQDN的基于RADIUS的身份验证尝试，从而产生过多的日志噪声，并引起对外部扫描或可能滥用VPN服务的担忧。

环境

- 思科安全接入平台
- 最初配置的远程访问VPN配置文件没有证书身份验证
- 为RA VPN配置的基于RADIUS的身份验证
- 具有可发现VPN配置文件的公共VPN租户配置

分辨率

解决方案包括了解身份验证流程行为以及实施基于证书的身份验证作为缓解策略。

观测行为的技术解释

由于以下部分中描述的技术原因，会发生过多的身份验证事件。

无证书要求的身份验证流程

当证书身份验证被禁用且使用基于RADIUS的RA VPN身份验证时，系统会记录“授权失败”尝试，因为系统首先根据在安全访问中同步的用户数据库检查用户名身份，并记录“授权失败”事件。这些事件被预期作为第一道防线，但在外部参与者尝试身份验证时可能会产生严重的日志噪声。

本地链路地址使用

日志中看到的169.254.x.x地址是RA VPN头端用于授权传入会话的内部/本地链路地址。这些地址代表内部系统行为，而不是租户中的AAA服务器配置错误。

VPN配置文件发现

当配置公共VPN租户ID时，VPN配置文件在UI下拉列表中列出，这样外部参与者可以更轻松地发现公共配置文件并将其作为身份验证尝试的目标。

立即缓解步骤

1. — 配置基于证书的身份验证。修改RA VPN配置文件以要求基于证书的身份验证。当需要证书身

份验证时，安全访问在身份验证流程中执行早期的证书检查。如果证书丢失，系统会在标准身份验证流程之前生成错误，并且“授权失败”事件不会以相同的方式记录。

2. — 验证缓解成效。在实施基于证书的身份验证后监控身份验证日志，以确认过度身份验证事件的减少。切换到基于证书的身份验证成功缓解了攻击并减少了日志噪声。

长期改进

为了解决根本问题，我们创建了两个功能请求：

- 功能请求1:添加选项以在添加公共VPN租户时隐藏或显示隧道组（VPN配置文件）列表，从而降低配置文件发现率。
- 功能请求2:添加配置选项以启用或禁用失败的RA VPN授权尝试的日志记录，为管理员提供对日志详细程度的控制。

此外，还会创建一个面向公众的文档，解释已记录的事件和身份验证行为，以帮助管理员了解正常的系统操作。

原因

过多的身份验证事件的根本原因是公共租户配置中的可发现VPN配置文件与不需要基于证书的身份验证时的身份验证流行为的组合。在没有证书要求的情况下使用基于RADIUS的身份验证时，系统会将所有“授权失败”尝试记录为其安全状态的一部分，包括来自发现VPN配置文件的外部参与者的尝试。日志中的本地链路地址代表RA VPN头端授权过程的正常内部系统行为，而不是配置错误。

相关内容

- [思科技术支持和下载](#)

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）。