使用一次性密码对具有RADIUS的ASA上的SSH身份验证故障进行故障排除

目录

问题

启用CiscoSSH堆栈时，安全外壳(SSH)使用一次性密码(OTP)访问具有远程身份验证拨入用户服务(RADIUS)的自适应安全设备(ASA)软件失败。

将生成以下系统日志消息：

```
Nov 14 2025 16:28:35: %ASA-6-113010: AAA challenge received for user from server .
Nov 14 2025 16:28:35: %ASA-4-109033: Authentication failed for admin user from . Interactive challenge
```

环境

当所有条件都匹配时，将观察以下症状：

- 在单情景或多情景模式下使用ASA保护防火墙1230。其他硬件平台也受到影响。
- RADIUS服务器用于SSH身份验证：

<#root>

device#

show run | i aaa

```
aaa-server RAD-OTP protocol radius
aaa-server RAD-OTP (management) host 192.0.2.1
aaa-server RAD-OTP (management) host 192.0.2.2
aaa authentication ssh console RAD-OTP
```

- RADIUS服务器请求并需要有效的OTP代码或质询才能成功进行身份验证。
- CiscoSSH堆栈在ASA上启用。
- 在版本9.19.1及更高版本中，CiscoSSH堆栈默认启用，并可使用no ssh stack cisco命令选择禁用。使用show ssh命令进行验证:

```
<#root>

device#

show ssh


ssh secure copy : ENABLED

ciscoSSH stack : DISABLED
```

- 在版本9.23.1及更高版本中，无法禁用或验证此堆栈。

分辨率

这些症状在内部实验中成功重现并在Cisco Bug ID CSCwt5790中跟踪。

在受影响的版本中使用以下解决方法选项之一：

- 对SSH连接使用本地身份验证。
- 在RADIUS服务器上，禁用ASA的OTP要求。
- 在早于9.23版本中，使用no ssh stack cisco命令禁用CiscoSSH堆栈。确保查看Cisco Secure Firewall ASA Series Command Reference， S Commands，并评估禁用CiscoSSH堆栈的潜在影响。

原因

身份验证失败的原因是Cisco Bug ID CSCwt57790。

相关内容

- Cisco Bug ID CSCwi04513
- Cisco Bug ID CSCwt57790
- 思科安全防火墙ASA系列命令参考，S命令

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）。