对会话重新身份验证后未触发的ISE无代理状态进行故障排除

目录

问题

身份服务引擎(ISE)3.3中的无代理状态功能在会话重新身份验证事件后无法触发。在初始身份验证期间，无代理状态工作正常，终端变得合规。但是，当发生重新身份验证时，终端会收到RADIUS记帐临时更新事件而不是记帐开始事件，导致无代理状态流不被调用。因此，终端匹配未知的终端安全评估策略，并保持未知的终端安全评估状态，从而影响受影响设备的网络访问。

问题表现在终端在重新身份验证后陷入“状态待定”或“未知”状态，在报告的环境中，1200个终端中有大约800个受到影响。日志分析显示，在重新身份验证期间，ISE收到agentlessEnabled=true的ACCOUNTING_UPDATE事件，但不会为现有会话ID重新调用状态流。

环境

- 身份服务引擎(ISE)版本3.3补丁4
- 有线802.1X身份验证，带MAC身份验证绕行(MAB)
- 已启用无代理状态配置
- 已配置会话重新身份验证计时器（420秒超时）
- 作为网络接入设备的Cisco Catalyst交换机
- 环境中约有1200个终端

分辨率

此行为在ISE中是预期行为，且是设计行为。无代理状态仅由RADIUS Accounting Start事件触发，并且当框架IP地址保持不变时，不会在会话重新身份验证期间由记帐临时更新事件重新调用。

技术分析

ISE NetAccessEventHandler代码路径仅对新的RADIUS Accounting-Start数据包重新处理无代理状态流。在重新身份验证期间，网络设备通常发送具有相同Acct-Session-Id的Accounting Interim-Update数据包，这会导致shouldInvokePostureFlow()函数返回false，从而防止状况重新评估。

显示行为的日志证据：

初始身份验证（无代理状态触发）：

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle

2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

重新身份验证（未触发无代理状态）：

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

建议的解决方法

要减轻此行为的影响，请配置终端安全评估租用设置，以在重新身份验证方案期间保持终端合规性：

步骤 1：在ISE终端安全评估策略中配置适当的终端安全评估租用持续时间，以确保终端在终端安全评估之间不会丢失网络访问权限。

步骤 2：根据组织的安全要求和重新身份验证频率，监控终端安全评估状态并调整租用计时器。

原因

这是思科Bug ID CSCwu48086中记录的预期行为。ISE中的无代理状态设计为仅在RADIUS记帐开始事件上触发，而不是由临时记帐更新事件触发。在会话重新身份验证期间，网络接入设备使用相

同的帧IP地址和会话ID发送记帐临时更新，这些更新不会重新调用无代理状态评估过程。ISE代码专门检查新会话（ACCOUNTING_START事件），然后启动无代理安全评估流程。

相关内容

- 思科漏洞ID CSCwu48086
- 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）。