使用IPS阻止设置的思科安全访问警告操作覆盖行为

目录

问题

在启用了IPS的Cisco Secure Access上测试访问策略(Internet Access)中的警告行为时，用户会遇到意外行为，其中显示“警告”(Warn)操作会覆盖IPS阻止设置。具体而言，当访问旨在触发IPS签名的URL时(SERVER-WEBAPP /etc/passwd file access attempt， GID-SID:1-1122)，系统会显示警告页面，并在用户确认后，尽管IPS配置为阻止流量，仍允许访问URL。

配置包括：

- 操作：隔离
- 入侵防御(IPS):enable
- IPS/阻止
- 签名：SERVER-WEBAPP /etc/passwd文件访问尝试
- GID-SID:1-1122

活动搜索日志显示冲突条目：

- IPS:(IPS:阻止)
- WEB:(网络：允许 — 显示警告页面)
- WEB:(网络：允许（在警告访问后）

环境

- 产品:思科安全互联网接入优势

- 技术：安全访问
- 配置了Internet访问和警告操作的访问策略
- 启用IPS，对特定签名执行阻止操作

分辨率

此行为在思科安全访问中被识别为缺陷，其中访问策略中的警告操作优先于IPS阻止设置。此问题影响访问策略警告操作和IPS阻止功能之间的交互。

验证步骤

要在您的环境中验证此行为，请执行以下操作：

步骤 1：使用警告操作配置访问策略并启用IPS阻止

- 将操作设置为使用警告行为隔离
- 启用入侵防御(IPS)
- 使用阻止操作配置IPS
- 应用特定签名(例如，SERVER-WEBAPP /etc/passwd文件访问尝试、GID-SID:1-1122)

步骤 2：通过访问触发IPS签名的URL测试配置

```
https://example.com/etc/passwd
```

步骤 3：观察行为

- 向用户显示警告页面
- 用户可以在确认警告后继续
- 无论IPS阻止配置如何，都将允许访问URL

步骤 4：检查活动搜索日志

- 验证IPS阻止和WEB允许条目的存在
- 确认存在冲突的日志条目指示缺陷

当前状态

此行为已被确认为缺陷，其中Warn操作会覆盖当前实施中设计时的IPS块设置。除GID-SID之外的IPS特征码也会出现相同行为：1-1122，表示这是系统问题，在配置警告操作时会影响所有IPS签名。

此缺陷的更正计划和时间表尚未确定。遇到此问题的组织应评估其安全策略，并在需要严格IPS阻止时考虑替代配置。

原因

根本原因是思科安全访问存在缺陷，其中访问策略警告操作处理优先于IPS块实施。此设计缺陷允许用户通过警告确认机制绕过IPS安全控制，从而在配置警告操作时有效取消IPS阻止功能。

Cisco Bug ID CSCwt39270（仅限注册用户）与此案例相关，但此Bug与观察到的Warn versus IPS行为之间的特定关系需要进一步调查。

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）。