在FTD升级期间，由于自定义策略检测，Snort引擎升级被阻止

目录

问题

在FMC管理的HA FPR-4115上从版本7.2升级到7.4.4期间，Snort引擎升级到Snort 3会被阻止，并显示错误消息，指示无法转换Snort 2自定义规则或使用自定义入侵或网络分析策略。特定错误消息表明："无法升级到Snort 3。设备至少使用一个自定义入侵策略或网络分析策略。" 更详细的故障消息引用无法转换Snort 2自定义规则，并指向/var/sf/htdocs/ips/snort.rej了解详细信息。问题是此错误是否会阻止迁移到Snort 3并影响检测功能。

环境

- 思科安全防火墙Firepower版本7.3
- Firepower管理中心(FMC)版本7.7.11
- 高可用性(HA)配置中的FTD设备
- Hardware:FPR-4115
- 升级路径:FTD 7.2至7.4.4
- 升级前的VDB为最新版本
- Objects > Intrusion Rules > Snort 2 All Rules下方的本地规则部分为空

分辨率

阻止Snort引擎升级的错误消息是与Cisco Bug ID CSCwn46794相关的有案可稽的行为，当不存在实际的自定义Snort 2规则时，该错误消息不代表功能拦截器。

验证步骤

第1步：验证自定义Snort 2规则状态

导航到FMC界面并检查自定义Snort 2规则：

```
Objects > Intrusion Rules > Snort 2 All Rules > Local Rules
```

第2步：确认VDB版本

在继续升级之前，请确保漏洞数据库(VDB)是最新版本。

第3步：查看错误详细信息

检查参考文件中的详细错误信息：

```
/var/sf/htdocs/ips/snort.rej
```

升级过程

当“本地规则”部分被确认为空（不存在自定义Snort 2规则）时，升级可以继续进行，尽管出现错误消息。在此方案中，阻止错误是误报，并不表示需要转换的实际自定义规则。

第1步：继续执行Snort 3升级

继续执行FTD升级到版本7.4.4（包括Snort 3引擎升级）的过程。

第2步：升级后验证

升级成功完成后，使用Snort 3引擎测试流量以确认预期行为。

第3步：监控系统性能

验证新的Snort 3引擎的检测功能是否按预期运行。

原因

升级阻止消息是与Cisco Bug ID CSCwn46794关联的已编档行为。此Bug会导致系统显示有关自定义入侵策略或网络分析策略的错误消息，即使不存在需要转换的实际自定义Snort 2规则。当“本地规则”部分为空时，该错误消息显示为误报，但系统升级前验证错误地识别了自定义策略的存在。

相关内容

- Cisco Bug ID CSCwn46794
- 思科漏洞ID CSCwk07199
- 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）。