

FMC入侵事件显示通用"Snort警报"消息

目录

问题

- 入侵事件不再在FMC GUI中显示描述性Snort规则消息，并导致可操作的警报信息丢失，影响安全监控功能。
- Echo回复的入侵事件消息通常显示如下：
- PROTOCOL-ICMP Echo Reply(1:408:8)

但是，此问题导致snort消息通常显示为“Snort警报”：

Snort Alert (1:408:8)

- 实际显示的规则名称和说明事件只是通用条目，例如Snort Alert(gid:sid:"rev)。

Overview Analysis Policies Devices Objects Integration			
Context Explorer	Unified Events	Connections	Intrusions Events
Files Hosts Users Correlation Advanced Search			
Events By Priority and Classification (switch workflow)			
Drilldown of Event, Priority, and Classification > Table View of Events > Packets			
No Search Constraints (Edit Search)			
Jump to...			
Message	Priority	Classification	
Snort Alert (1:51390:2)	medium	Attempted Information Leak	
Snort Alert (1:1000074:6)	low	Generic ICMP Event	
Snort Alert (1:1000087:5)	high	Web Application Attack	
Snort Alert (1:41421:2)	high	Web Application Attack	
Snort Alert (1:63309:1)	high	Web Application Attack	
Snort Alert (1:16431:6)	high	Web Application Attack	
Snort Alert (1:58726:7)	high	Attempted User Privilege Gain	
Snort Alert (1:58737:5)	high	Attempted User Privilege Gain	
Snort Alert (1:58723:6)	high	Attempted User Privilege Gain	
Snort Alert (1:58743:6)	high	Attempted User Privilege Gain	
Snort Alert (1:58742:8)	high	Attempted User Privilege Gain	
Snort Alert (1:65554:1)	high	Attempted User Privilege Gain	
Snort Alert (1:58744:6)	high	Attempted User Privilege Gain	
Snort Alert (1:58722:5)	high	Attempted User Privilege Gain	
Snort Alert (3:58806:4)	high	Attempted User Privilege Gain	

- 在Packet视图中，在Event Information中显示相同类型的消息，其中Rule Unavailable。

The screenshot shows the Cisco FMC Analysis interface. The top navigation bar includes Overview, Analysis (selected), Policies, Devices, Objects, and Integration. Below this, there are tabs for Context Explorer, Unified Events, Connections, and Intrusions > Events (selected). The main heading is 'Events By Priority and Classification' with a '(switch workflow)' link. Below the heading are links for 'Drilldown of Event, Priority, and Classification', 'Table View of Events', and 'Packets'. A search bar is present with 'Search Constraints' and links for 'Edit Search' and 'Save Search'. The 'Event Information' section is expanded, showing a table of event details. The 'Message' field is highlighted with a red box, showing 'Snort Alert (1:51390:2)'. The 'Rule' field at the bottom is also highlighted with a red box, showing 'Rule Unavailable'.

Message	Snort Alert (1:51390:2)
Time	2026-05-05 15:37:39
Classification	Attempted Information Leak
Priority	medium
Ingress Security Zone	
Device	
Ingress Interface	
Source IP	
Source Port / ICMP Type	60402 / tcp
Source Country	USA
Destination IP	
Destination Port / ICMP Code	80 (http) / tcp
Destination Country	USA
HTTP Hostname	
HTTP URI	
Intrusion Policy	
Access Control Policy	
Access Control Rule	
Rule	Rule Unavailable

- 此外，从FMC导出到SIEM系统的系统日志事件包含以下字段的空值：

- sig_id
- signature_msg
- signature_desc

- FMC消息日志显示与事件消息相关的多个入侵事件的重复错误：

Apr 10 23:28:56 FMC SF-IMS[21500]: [21500] EventStreamer child(192.X.X.210):sfestreamer [WARN] Unavailable

- 此问题会影响从受管传感器进入FMC的所有入侵事件，并在正常的FMC Sourcefire规则更新(SRU)和本地安全包(LSP)更新中持续出现。

环境

- 首次出现在高可用性(HA)中运行FMC 7.2.11(build 313)的思科安全防火墙管理中心2600上
- 正在应用常规SRU/LSP、GeoDB和VDB更新，但未能解决此问题

分辨率

通过强制重新安装Sourcefire规则更新(SRU)软件包以正确重建Snort签名消息数据库可以解决此问题。

1. — 访问FMC CLI并验证最新安装的SRU软件包：

<#root>

> expert

admin@FMC:~\$ sudo su

root@FMC:/Volume/home/admin# ls -halts /var/sf/SRU/ | grep SRU-2026-05

43M	-rw-r--r--	1	www	www	43M	May 27 04:02	Cisco_Firepower_SRU-2026-05-26-001-vrt.sh.REL.tar
43M	-rw-r--r--	1	www	www	43M	May 22 04:02	Cisco_Firepower_SRU-2026-05-20-001-vrt.sh.REL.tar
43M	-rw-r--r--	1	www	www	43M	May 20 04:02	Cisco_Firepower_SRU-2026-05-19-001-vrt.sh.REL.tar
43M	-rw-r--r--	1	www	www	43M	May 13 04:03	Cisco_Firepower_SRU-2026-05-12-001-vrt.sh.REL.tar
43M	-rw-r--r--	1	www	www	43M	May 8 04:03	Cisco_Firepower_SRU-2026-05-06-001-vrt.sh.REL.tar
43M	-rw-r--r--	1	www	www	43M	May 6 04:03	Cisco_Firepower_SRU-2026-05-04-001-vrt.sh.REL.tar

2. — 执行强制重新安装SRU软件包：

<#root>

root@FMC:/Volume/home/admin#

install_update.pl --detach /var/sf/SRU/Cisco_Firepower_SRU-2026-05-26-001-vrt.sh.REL.tar --force

3. — 使用此命令跟踪安装进度：

<#root>

root@FMC:/Volume/home/admin#

tail -f /var/log/sf/sru-2026-05-26-001-vrt/status.log & tail -f /var/log/sf/sru-2026-05-26-001-vrt/sru.1

[260528 12:43:34] **** Finish POST phase

[260528 12:43:34] *****

[260528 12:43:34] COMPLETED post/999_finish.sh

[260528 12:43:34]

[260528 12:43:34] Lock //tmp/sru.lock for force install removed successfully.

```
[260528 12:43:34] Pruning logs and old installs
[260528 12:43:34]
[260528 12:43:34] #####
[260528 12:43:34] # FORCE COMPLETE
[260528 12:43:34] #####
ui:[63%] Running script installer/602_log_package.pl...
ui:[68%] Running script installer/900_update_version.sh...
ui:[74%] Running script installer/999_finish.sh...
ui:[79%] Running script post/000_start.sh...
ui:[84%] Running script post/500_copy_contents.sh...
ui:[89%] Running script post/900_iru_log_finish.pl...
ui:[95%] Running script post/999_finish.sh...
ui:[100%] The force install completed successfully.
ui:The force install has completed.
state:finished
```



注意：SRU安装可能需要20分钟才能完成，并且可能以一定的百分比滞留数分钟。此行为是正常的。

4:强制SRU重新安装成功完成后：

- 监控FMC入侵事件页面以获取新事件
- 确认新的入侵事件显示正确的Snort规则消息而不是通用“Snort警报”条目
- 确认系统日志导出到SIEM系统现在包含填充的签名字段



提示：此修复不具追溯性。以前生成的没有正确消息的事件保持不变，但所有新的入侵事件必须正确显示正确的Snort规则消息并正确填充系统日志字段。

原因

FMC中的缺陷导致Snort签名消息数据库损坏和/或不同步，从而阻止FMC解析和填充入侵事件中的Snort规则元数据。此行为在Cisco Bug ID CSCwu63768下跟踪。

此问题被认为是由之前的SRU/LSP更新安装不正确引起的，即使安装可以成功也是如此。证据显示签名元数据存在于传感器级别（由GID:SID:REV标识的事件），但由于数据库损坏而无法由FMC解析以进行正确的消息显示或系统日志导出。

相关内容

- [思科漏洞ID CSCwu63768](#)
- [Sourcefire规则更新下载](#)
- [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）。