

FMC入侵事件顯示通用"Snort警報"訊息

目錄

問題

- 入侵事件不再在FMC GUI中顯示描述性Snort規則消息，從而導致可操作的警報資訊丟失，並影響安全監控功能。
- Echo回覆的入侵事件消息通常顯示如下：
- PROTOCOL-ICMP Echo Reply(1:408:8)

但是，該問題導致snort消息更一般地顯示為「Snort警報」：

Snort Alert (1:408:8)

- 實際顯示的規則名稱和說明事件只是通用條目，如Snort警報(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檢視中，相同型別的消息出現在Event Information中，其中Rule Unavailable。

Overview **Analysis** Policies Devices Objects Integration

Context Explorer Unified Events Connections **Intrusions ▶ Events**

Events By Priority and Classification (switch workflow)

[Drilldown of Event, Priority, and Classification](#) > [Table View of Events](#) > **Packets**

▶ Search Constraints ([Edit Search](#) [Save Search](#))

Event Information ▼

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，從FMC匯出到SIEM系統的系統日誌事件包含以下欄位的空值：
 - sig_id
 - 簽名消息
 - signature_desc
- FMC消息日誌顯示與事件消息有關的多個入侵事件的重複錯誤：

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

- 此問題會影響從受管感測器進入FMC的所有入侵事件，並在正常的FMC Sourcefire規則更新(SRU)和本地安全包(LSP)更新中持續出現。

環境

- 首次出現在高可用性(HA)中運行FMC 7.2.11(build 313)的Cisco Secure Firewall Management Center 2600上

- 正在應用常規SRU/LSP、GeoDB和VDB更新，但未解決此問題

解析

通過執行Sourcefire規則更新(SRU)包的強制重新安裝以正確重建Snort簽名消息資料庫可以解決此問題。

1. — 訪問FMC CLI並驗證最新安裝的SRU軟體包：

```
<#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. — 執行強制重新安裝SRU軟體包：

```
<#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. — 使用以下命令跟蹤安裝進度：

```
<#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.
```

```
[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
```



附註：SRU安裝可能需要20分鐘才能完成，並且可能以一定的百分比滯留數分鐘。這是正常行為。

4:強制SRU重新安裝成功完成後：

- 監視FMC入侵事件頁面以獲取新事件
- 驗證新的入侵事件是否顯示正確的Snort規則消息而不是通用「Snort警報」條目
- 確認系統日誌匯出到SIEM系統現在包含填充的簽名欄位



提示：此修復程式沒有追溯功能。以前生成的沒有正確消息的事件將保持不變，但所有新的入侵事件都必須顯示正確的Snort規則消息並正確填充系統日誌欄位。

原因

FMC中的缺陷導致Snort簽名消息資料庫的損壞和/或不同步，從而使FMC無法在入侵事件中解析和填充Snort規則後設資料。此行為在思科錯誤ID CSCwu63768下跟蹤。

此問題被認為是由先前的SRU/LSP更新安裝不正確觸發的，即使安裝可以成功。證據顯示簽名後設資料存在於感測器級別（事件由GID:SID:REV標識），但由於資料庫損壞而無法由FMC解析以進行

正確的消息顯示或系統日誌匯出。

相關內容

- [思科錯誤ID CSCwu63768](#)
- [Sourcefire規則更新下載](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。