

FMC Intrusion Events Display Generic "Snort Alert" Messages

Contents

Issue

- Intrusion events no longer display descriptive Snort rule messages in the FMC GUI and results in loss of actionable alerting information and impacts security monitoring capabilities.
- An intrusion event message for Echo replies typically shows like this:

- **PROTOCOL-ICMP Echo Reply (1:408:8)**

However, the issue causes the snort messages to appear more generically as "Snort Alert":

Snort Alert (1:408:8)

- The actual rule names and descriptions events display are only generic entries such as **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

- In the Packet view, the same type of message appears with **Rule Unavailable** in the Event Information.

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

- Additionally, syslog events exported from FMC to SIEM systems contain empty values for these fields:
 - `sig_id`

- **signature_msg**
- **signature_desc**
- FMC messages log shows repeating errors for multiple intrusion events regarding event messages:

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

- The issue affects all intrusion events coming into the FMC from the managed sensors and persists across normal FMC Sourcefire Rule Update (SRU) and Local Security Package (LSP) updates.

Environment

- First seen on Cisco Secure Firewall Management Center 2600 running FMC 7.2.11 (build 313) in High Availability (HA)
- Regular SRU/LSP, GeoDB, and VDB updates were being applied but did not resolve the issue

Resolution

The issue is resolved by performing a forced reinstallation of the Sourcefire Rule Update (SRU) package to rebuild the Snort signature message database correctly.

1.- Access the FMC CLI and verify the latest installed SRU package:

```
<#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.- Execute the forced reinstallation of the SRU package:

```
<#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.- Track the installation progress using this command:

```
<#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
```



Note: The SRU installation can take up to 20 minutes to complete and can appear to stick at certain percentages for several minutes. This is normal behavior.

4: After the forced SRU reinstallation completes successfully:

- Monitor the FMC intrusion events page for new events
- Verify that new intrusion events display proper Snort rule messages instead of generic "Snort Alert" entries

- Confirm that syslog exports to SIEM systems now contain populated signature fields
-



Tip: This fix is not retroactive. Previously generated events without proper message remains unchanged, but all new intrusion events must display correct Snort rule messages and populate syslog fields properly.

Cause

A defect in the FMC caused corruption and/or desynchronization of the Snort signature message database, preventing FMC from resolving and populating Snort rule metadata in intrusion events. This behavior is tracked under **Cisco bug ID CSCwu63768**.

The issue is believed to be triggered by the improper installation of a previous SRU/LSP update, even though the installation can be successful. Evidence showed that signature metadata existed at the sensor level (events identified by GID:SID:REV) but could not be resolved by FMC for proper message display or syslog export due to database corruption.

Related Content

- [Cisco bug ID CSCwu63768](#)
- [Sourcefire Rule Update Downloads](#)
- [Cisco Technical Support & Downloads](#)