

"Snort Alert" generico visualizzato dagli eventi di intrusione di FMC Messaggi

Sommario

Problema

- Gli eventi di intrusione non visualizzano più i messaggi descrittivi delle regole di snort nell'interfaccia utente grafica di FMC e determinano la perdita di informazioni di avviso attivabili e influiscono sulle funzionalità di monitoraggio della sicurezza.
- Un messaggio di evento intrusione per le risposte Eco è in genere simile al seguente:
- Risposta echo PROTOCOL-ICMP (1:408:8)

Tuttavia, questo problema fa sì che i messaggi snort appaiano più genericamente come "Snort Alert":

Snort Alert (1:408:8)

- I nomi effettivi delle regole e gli eventi di descrizione visualizzati sono solo voci generiche, ad esempio Avviso snort (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

- Nella vista Pacchetto, lo stesso tipo di messaggio viene visualizzato con Regola non disponibile in Informazioni evento.

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

- Inoltre, gli eventi syslog esportati da FMC nei sistemi SIEM contengono valori vuoti per questi campi:
 - sig_id

- messaggio_firma
- descrizione_firma
- Nel registro dei messaggi di FMC vengono visualizzati errori ripetuti per più eventi di intrusione relativi ai messaggi di evento:

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

- Il problema interessa tutti gli eventi di intrusione provenienti dai sensori gestiti e persiste nei normali aggiornamenti SRU (Sourcefire Rule Update) e LSP (Local Security Package) di FMC.

Ambiente

- Visualizzato per la prima volta su Cisco Secure Firewall Management Center 2600 con FMC 7.2.11 (build 313) in alta disponibilità (HA)
- Gli aggiornamenti SRU/LSP, GeoDB e VDB regolari sono stati applicati ma non hanno risolto il problema

Risoluzione

Il problema viene risolto eseguendo una reinstallazione forzata del pacchetto Sourcefire Rule Update (SRU) per ricostruire correttamente il database dei messaggi di firma Snort.

1.- Accedere alla CLI di FMC e verificare l'ultimo pacchetto SRU installato:

```
<#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.- Eseguire la reinstallazione forzata del pacchetto SRU:

<#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.- Controllare lo stato dell'installazione utilizzando questo comando:

<#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_iwu_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
```



Nota: Il completamento dell'installazione dell'unità SRU può richiedere fino a 20 minuti e può sembrare che si attenga a determinate percentuali per diversi minuti. Si tratta di un comportamento normale.

4: Dopo il completamento della reinstallazione SRU forzata:

- Monitoraggio della pagina Eventi intrusione FMC per nuovi eventi
- Verificare che i nuovi eventi di intrusione visualizzino i messaggi della regola Snort appropriati anziché le voci generiche di "Avviso snort"
- Confermare che le esportazioni syslog nei sistemi SIEM ora contengono campi di firma popolati



Suggerimento: Questa correzione non è retroattiva. Gli eventi generati in precedenza senza il messaggio appropriato rimangono invariati, ma tutti i nuovi eventi di intrusione devono visualizzare i messaggi delle regole Snort corretti e popolare correttamente i campi syslog.

Causa

Un difetto nel FMC ha causato il danneggiamento e/o la desincronizzazione del database dei messaggi delle firme Snort, impedendo al FMC di risolvere e popolare i metadati delle regole Snort negli eventi di intrusione. Questo comportamento viene registrato in Cisco bug ID CSCwu63768.

Il problema si ritiene causato dall'installazione non corretta di un precedente aggiornamento SRU/LSP, anche se l'installazione può avere esito positivo. È stato dimostrato che i metadati della firma esistevano a livello di sensore (eventi identificati da GID:SID:REV) ma non potevano essere risolti da FMC per la corretta visualizzazione dei messaggi o l'esportazione del syslog a causa di un danneggiamento del database.

Contenuto correlato

- [ID bug Cisco CSCwu63768](#)
- [Download per l'aggiornamento delle regole Sourcefire](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).