

FMC Intrusion Events Display Generic "Snort Alert" Mensajes

Contenido

Problema

- Los eventos de intrusión ya no muestran mensajes descriptivos de reglas Snort en la GUI de FMC y provocan la pérdida de información de alertas procesables, lo que afecta a las capacidades de supervisión de la seguridad.
- Un mensaje de evento de intrusión para las respuestas de eco suele mostrarse de la siguiente manera:
- PROTOCOL-ICMP Echo Reply (1:408:8)

Sin embargo, el problema hace que los mensajes de snort aparezcan más genéricamente como "Alerta de Snort":

Snort Alert (1:408:8)

- Los nombres de reglas reales y las descripciones de eventos que se muestran son solo entradas genéricas como Alerta de 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

- En la vista de paquete, aparece el mismo tipo de mensaje con Regla no disponible en Información del 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

- Además, los eventos syslog exportados de FMC a sistemas SIEM contienen valores vacíos para estos campos:
 - sig_id

- signature_msg
- signature_desc
- El registro de mensajes de FMC muestra errores repetidos de varios eventos de intrusión relacionados con mensajes de eventos:

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

- El problema afecta a todos los eventos de intrusión que llegan al FMC desde los sensores gestionados y persiste en las actualizaciones normales de la actualización de reglas (SRU) y del paquete de seguridad local (LSP) de FMC Sourcefire.

Entorno

- Visto por primera vez en Cisco Secure Firewall Management Center 2600 con FMC 7.2.11 (build 313) en alta disponibilidad (HA)
- Se estaban aplicando actualizaciones regulares de SRU/LSP, GeoDB y VDB, pero no resolvieron el problema

Resolución

El problema se resuelve realizando una reinstalación forzada del paquete de actualización de reglas de Sourcefire (SRU) para reconstruir correctamente la base de datos de mensajes de firma de Snort.

1.- Acceder a la CLI de la FMC y verificar el último paquete de SRU instalado:

```
<#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.- Ejecutar la reinstalación forzada del paquete 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.- Seguimiento del progreso de la instalación utilizando este 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: La instalación de la SRU puede tardar hasta 20 minutos en completarse y parece que se mantiene en ciertos porcentajes durante varios minutos. Esto es normal.

4: Después de que la reinstalación de SRU forzada se complete con éxito:

- Supervise la página de eventos de intrusión de FMC para ver los nuevos eventos
- Verifique que los nuevos eventos de intrusión muestren mensajes de regla Snort adecuados en lugar de entradas genéricas de "alerta Snort"
- Confirme que las exportaciones de syslog a los sistemas SIEM ahora contengan campos de firma rellenos



Consejo: Esta corrección no es retroactiva. Los eventos generados anteriormente sin el mensaje adecuado permanecen sin cambios, pero todos los nuevos eventos de intrusión deben mostrar mensajes de regla Snort correctos y rellenar correctamente los campos de syslog.

Causa

Un defecto en el FMC causaba daños y/o desincronización de la base de datos de mensajes de firma de Snort, lo que impedía a FMC resolver y rellenar los metadatos de regla de Snort en eventos de intrusión. Este comportamiento se rastrea bajo el Id. de bug Cisco CSCwu63768.

Se cree que el problema es provocado por la instalación incorrecta de una actualización anterior de SRU/LSP, aunque la instalación puede ser exitosa. La evidencia mostró que los metadatos de la firma existían a nivel del sensor (eventos identificados por GID:SID:REV) pero no pudieron ser resueltos por FMC para la visualización correcta de mensajes o la exportación de syslog debido a la corrupción de la base de datos.

Contenido relacionado

- [ID de bug de Cisco CSCwu63768](#)
- [Descargas de actualización de reglas de Sourcefire](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).