

FMC Intrusion Events Display Generic " ; Snort Alert" ; Messages

Table des matières

Problème

- Les événements d'intrusion n'affichent plus de messages de règles Snort descriptifs dans l'interface utilisateur graphique de FMC et entraînent la perte d'informations d'alerte exploitables et ont un impact sur les fonctionnalités de surveillance de la sécurité.
- Un message d'événement d'intrusion pour les réponses Echo se présente généralement comme suit :
- Réponse d'écho PROTOCOLE-ICMP (1:408:8)

Cependant, le problème fait apparaître les messages de reniflement de façon plus générique sous le nom de « Snort Alert » :

Snort Alert (1:408:8)

- Les noms de règles et les descriptions réels des événements affichés sont uniquement des entrées génériques telles que Alerte de renversement (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

- Dans la vue Packet, le même type de message apparaît avec Rule Unavailable dans 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

- En outre, les événements syslog exportés de FMC vers les systèmes SIEM contiennent des valeurs vides pour ces champs :
 - sig_id

- signature_msg
- desc_signature
- Le journal des messages FMC affiche les erreurs répétées pour plusieurs événements d'intrusion concernant les messages d'événement :

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

- Le problème affecte tous les événements d'intrusion arrivant dans le FMC à partir des capteurs gérés et persiste lors des mises à jour normales de la règle Sourcefire (SRU) et du package de sécurité local (LSP) du FMC.

Environnement

- Première vue sur Cisco Secure Firewall Management Center 2600 exécutant FMC 7.2.11 (build 313) en haute disponibilité (HA)
- Des mises à jour régulières SRU/LSP, GeoDB et VDB étaient appliquées, mais n'ont pas résolu le problème

Résolution

Le problème est résolu en effectuant une réinstallation forcée du package Sourcefire Rule Update (SRU) pour reconstruire correctement la base de données des messages de signature Snort.

1.- Accédez à l'interface de ligne de commande du FMC et vérifiez le dernier package SRU installé :

```
<#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.- Exécutez la réinstallation forcée du package 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.- Suivez la progression de l'installation à l'aide de cette commande :

<#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

```



Remarque : L'installation de l'unité SRU peut prendre jusqu'à 20 minutes et peut sembler rester à certains pourcentages pendant plusieurs minutes. Ce comportement est normal.

4: Une fois la réinstallation forcée SRU terminée avec succès :

- Surveiller la page des événements d'intrusion FMC pour les nouveaux événements
- Vérifiez que les nouveaux événements d'intrusion affichent les messages de règle Snort appropriés au lieu des entrées génériques « Alerte Snort »
- Vérifiez que les exportations Syslog vers les systèmes SIEM contiennent désormais des champs de signature renseignés



Conseil : Ce correctif n'est pas rétroactif. Les événements précédemment générés sans message approprié restent inchangés, mais tous les nouveaux événements d'intrusion doivent afficher les messages de règle Snort corrects et remplir correctement les champs Syslog.

Motif

Un défaut dans le FMC a entraîné la corruption et/ou la désynchronisation de la base de données de messages de signature Snort, empêchant le FMC de résoudre et de remplir les métadonnées de règle Snort dans les événements d'intrusion. Ce comportement est suivi sous l'ID de bogue Cisco CSCwu63768.

Le problème est probablement déclenché par l'installation incorrecte d'une mise à jour SRU/LSP précédente, même si l'installation peut réussir. Des éléments de preuve ont montré que des métadonnées de signature existaient au niveau du capteur (événements identifiés par GID:SID:REV) mais n'ont pas pu être résolues par FMC pour un affichage correct des messages ou une exportation Syslog en raison d'une corruption de la base de données.

Autres informations utiles

- [ID de bogue Cisco CSCwu63768](#)
- [Téléchargements de mises à jour de règles Sourcefire](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.