

FMC Intrusion Events Gebeurtenissen

Generieke " weergegeven; Waarschuwing"

snurken; Berichten

Inhoud

uitgifte

- Inbraakgebeurtenissen geven geen beschrijvende Snoort-regelberichten meer weer in de FMC-gebruikersinterface en leiden tot verlies van bruikbare waarschuwingsinformatie en de beveiligingsbewakingsmogelijkheden.
- Een bericht over een inbraakgebeurtenis voor Echo-antwoorden ziet er doorgaans als volgt uit:
- PROTOCOL-ICMP Echo Reply (1:408:8)

Het probleem zorgt er echter voor dat de snortberichten meer algemeen worden weergegeven als "Snort Alert":

Snort Alert (1:408:8)

- De werkelijke regelnamen en beschrijvingen die worden weergegeven, zijn alleen generieke vermeldingen zoals Sneeuwbericht (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 de pakketweergave wordt hetzelfde type bericht weergegeven met Regel niet beschikbaar in de gebeurtenisinformatie.

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

- Bovendien bevatten syslog-gebeurtenissen die worden geëxporteerd van FMC naar SIEM-systemen lege waarden voor deze velden:
 - SIG_ID

- signature_msg
- signature_desc
- FMC-berichtenlog toont herhaalde fouten voor meerdere inbraakgebeurtenissen met betrekking tot gebeurtenisberichten:

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

- Het probleem is van invloed op alle inbraakgebeurtenissen die vanuit de beheerde sensoren in het FMC worden ingevoerd en blijft bestaan bij normale updates van de broncode van het FMC (SRU) en het lokale beveiligingspakket (LSP).

milieu

- Voor het eerst gezien op Cisco Secure Firewall Management Center 2600 met FMC 7.2.11 (build 313) in High Availability (HA)
- Er werden regelmatige SRU/LSP-, GeoDB- en VDB-updates toegepast, maar deze hebben het probleem niet opgelost

resolutie

Het probleem wordt opgelost door een geforceerde herinstallatie van het Sourcefire Rule Update (SRU)-pakket uit te voeren om de Snort-handtekeningberichtendatabase correct opnieuw samen te stellen.

1.- Toegang tot de FMC CLI en verificatie van het meest recente geïnstalleerde SRU-pakket:

```
<#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.- De gedwongen herinstallatie van het SRU-pakket uitvoeren:

<#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.- Volg de voortgang van de installatie met behulp van deze opdracht:

<#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
```



Opmerking: de SRU-installatie kan tot 20 minuten duren en kan enkele minuten op bepaalde percentages lijken te blijven. Dit is normaal gedrag.

4: Nadat de geforceerde SRU-herinstallatie met succes is voltooid:

- Bewaak de pagina Intrusion Events van de FMC voor nieuwe gebeurtenissen
- Controleer of nieuwe inbraakgebeurtenissen de juiste Snort-regelberichten weergeven in plaats van algemene "Snort Alert"-vermeldingen
- Bevestig dat syslog-exporten naar SIEM-systemen nu ingevulde handtekeningvelden bevatten



Tip: deze fix is niet retroactief. Eerder gegenereerde gebeurtenissen zonder het juiste bericht blijven ongewijzigd, maar alle nieuwe inbraakgebeurtenissen moeten correcte Snort-regelberichten weergeven en syslog-velden correct invullen.

Oorzaak

Een defect in het FMC veroorzaakte corruptie en/of desynchronisatie van de database met berichten over de Snoort-handtekening, waardoor het FMC niet in staat was metagegevens over de Snoort-regel op te lossen en in te vullen bij inbraakgebeurtenissen. Dit gedrag wordt gevolgd onder Cisco bug ID CSCwu63768.

Het probleem wordt verondersteld te worden veroorzaakt door de onjuiste installatie van een eerdere SRU / LSP-update, hoewel de installatie succesvol kan zijn. Bewijs toonde aan dat handtekening metadata bestond op het sensor niveau (gebeurtenissen geïdentificeerd door GID: SID: REV), maar kon niet worden opgelost door FMC voor de juiste bericht weergave of syslog export als gevolg van database corruptie.

Gerelateerde inhoud

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.