

FMC-Angriffssereignisse zeigen generische "Snort-Warnung" an Nachrichten

Inhalt

Problem

- Angriffssereignisse zeigen in der FMC-GUI keine beschreibenden Snort-Regelmeldungen mehr an, was zum Verlust von aussagekräftigen Warninformationen und zu Beeinträchtigungen der Sicherheitsüberwachungsfunktionen führt.
- Eine Meldung über ein Angriffssereignis für Echo-Antworten sieht in der Regel folgendermaßen aus:
- PROTOCOL-ICMP Echo Reply (1:408:8)

Das Problem führt jedoch dazu, dass die Snort-Meldungen generischer als "Snort Alert" angezeigt werden:

Snort Alert (1:408:8)

- Die tatsächlich angezeigten Regelnamen und -beschreibungen sind nur generische Einträge wie 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 der Paketansicht wird derselbe Meldungstyp angezeigt, wobei in den Ereignisinformationen Regel nicht verfügbar ist.

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

- Darüber hinaus enthalten Syslog-Ereignisse, die von FMC zu SIEM-Systemen exportiert werden, leere Werte für die folgenden Felder:
 - sig_id

- Signatur_msg
- Signatur_Beschreibung
- Das FMC-Nachrichtenprotokoll zeigt wiederholte Fehler bei mehreren Angriffsereignissen in Bezug auf Ereignismeldungen:

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

- Das Problem betrifft alle Angriffsversuche, die von den verwalteten Sensoren in das FMC eingehen, und besteht auch bei normalen Sourcefire Rule Update (SRU)- und Local Security Package (LSP)-Updates des FMC fort.

Umwelt

- Erster Einsatz auf dem Cisco Secure Firewall Management Center 2600 mit FMC 7.2.11 (Build 313) in High Availability (HA)
- Regelmäßige SRU/LSP-, GeoDB- und VDB-Updates wurden angewendet, konnten das Problem jedoch nicht beheben.

Auflösung

Das Problem wird durch eine erzwungene Neuinstallation des Sourcefire Rule Update (SRU)-Pakets behoben, um die Snort-Signaturnachrichtendatenbank ordnungsgemäß neu zu erstellen.

1.- Zugriff auf die FMC-CLI und Überprüfung des zuletzt installierten SRU-Pakets:

```
<#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.- Führen Sie die erzwungene Neuinstallation des SRU-Pakets aus:

<#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.- Verfolgen Sie den Installationsfortschritt mit dem folgenden Befehl:

<#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
```



Anmerkung: Die SRU-Installation kann bis zu 20 Minuten in Anspruch nehmen und bei bestimmten Prozentsätzen mehrere Minuten lang beibehalten werden. Das ist normales Verhalten.

4: Nachdem die erzwungene SRU-Neuinstallation erfolgreich abgeschlossen wurde:

- Überwachen der FMC-Seite mit Angriffsversuchen auf neue Ereignisse
- Vergewissern Sie sich, dass bei neuen Angriffsereignissen korrekte Snort-Regelmeldungen statt generischer "Snort Alert"-Einträge angezeigt werden.
- Bestätigen, dass die Syslog-Exporte in SIEM-Systeme jetzt ausgefüllte Signaturfelder enthalten



Tipp: Diese Korrektur ist nicht rückwirkend. Zuvor generierte Ereignisse ohne ordnungsgemäße Meldung bleiben unverändert, aber alle neuen Angriffsversuche müssen die richtigen Snort-Regelmeldungen anzeigen und die Syslog-Felder ordnungsgemäß ausfüllen.

Ursache

Ein Fehler im FMC hat zu einer Beschädigung und/oder Desynchronisierung der Snort-Signaturnachrichtendatenbank geführt und verhindert, dass FMC Snort-Regelmetadaten in Angriffsereignissen auflösen und ausfüllen kann. Dieses Verhalten wird unter der Cisco Bug-ID CSCwu63768 verfolgt.

Das Problem wird vermutlich durch die unsachgemäße Installation eines vorherigen SRU/LSP-Updates ausgelöst, obwohl die Installation erfolgreich sein kann. Es hat sich gezeigt, dass Signaturmetadaten auf Sensorebene vorhanden waren (Ereignisse, die von GID:SID:REV identifiziert wurden), von FMC jedoch nicht für eine ordnungsgemäße Nachrichtenanzeige oder einen Syslog-Export aufgrund einer Datenbankbeschädigung aufgelöst werden konnten.

Verwandte Inhalte

- [Cisco Bug-ID CSCwu63768](#)
- [Downloads von Sourcefire-Regelaktualisierungen](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.