

FMC 침입 이벤트는 일반 "Snort 경고"를 표시합니다. 메시지

목차

문제

- 침입 이벤트는 FMC GUI에서 더 이상 설명적 Snort 규칙 메시지를 표시하지 않으며 실행 가능한 알림 정보가 손실되고 보안 모니터링 기능에 영향을 미칩니다.
- 에코 회신에 대한 침입 이벤트 메시지는 일반적으로 다음과 같이 표시됩니다.
- PROTOCOL-ICMP Echo Reply(1:408:8)

그러나 이 문제로 인해 snort 메시지가 더 일반적으로 "Snort Alert"로 표시됩니다.

Snort Alert (1:408:8)

- 이벤트가 표시하는 실제 규칙 이름 및 설명은 Snort Alert(gid:sid:"rev)와 같은 일반 항목뿐입니다.

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](#)

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

- Packet(패킷) 보기에서는 동일한 유형의 메시지가 Event Information(이벤트 정보)에 Rule Unavailable(규칙 사용 불가)과 함께 나타납니다.

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

- 또한 FMC에서 SIEM 시스템으로 내보낸 syslog 이벤트에는 다음 필드에 대한 빈 값이 포함됩니다.
 - sig_id

- 서명 메시지
- 서명 설명
- FMC 메시지 로그는 이벤트 메시지와 관련된 여러 침입 이벤트에 대한 반복 오류를 표시합니다.

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

- 이 문제는 관리되는 센서에서 FMC로 들어오는 모든 침입 이벤트에 영향을 미치며 정상적인 FMC SRU(Sourcefire Rule Update) 및 LSP(Local Security Package) 업데이트 전반에 걸쳐 지속됩니다.

환경

- HA(High Availability)에서 FMC 7.2.11(빌드 313)을 실행하는 Cisco Secure Firewall Management Center 2600에서 처음 확인
- 일반 SRU/LSP, GeoDB 및 VDB 업데이트가 적용되었지만 문제가 해결되지 않았습니다.

해결

Sourcefire SRU(Rule Update) 패키지를 강제로 다시 설치하여 Snort 서명 메시지 데이터베이스를 올바르게 다시 구축하면 문제가 해결됩니다.

1.- FMC CLI에 액세스하여 최신 SRU 패키지를 확인합니다.

<#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.- SRU 패키지의 강제 재설치를 실행합니다.

<#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.- 다음 명령을 사용하여 설치 진행률을 추적합니다.

<#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
```



참고: SRU 설치를 완료하는 데 최대 20분이 소요될 수 있으며 몇 분 동안 특정 백분율로 유지되는 것처럼 보일 수 있습니다. 이는 정상적인 동작입니다.

4: 강제 SRU 재설치가 성공적으로 완료되면 다음을 수행합니다.

- FMC 침입 이벤트 페이지에서 새 이벤트를 모니터링합니다
- 새 침입 이벤트가 일반 "Snort Alert" 항목 대신 적절한 Snort 규칙 메시지를 표시하는지 확인합니다.
- Syslog를 SIEM 시스템으로 내보내기에 이제 채워진 시그니처 필드가 포함되었는지 확인합니다



팁: 이 수정은 소급되지 않습니다. 적절한 메시지가 없는 이전에 생성된 이벤트는 변경되지 않지만 모든 새로운 침입 이벤트는 올바른 Snort 규칙 메시지를 표시하고 syslog 필드를 올바르게 채워야 합니다.

원인

FMC의 결함으로 인해 Snort 서명 메시지 데이터베이스의 손상 및/또는 동기화 취소가 발생하여 FMC에서 침입 이벤트의 Snort 규칙 메타데이터를 확인하고 채우지 못했습니다. 이 동작은 Cisco 버그 ID CSCwu63768에서 추적됩니다.

이전 SRU/LSP 업데이트를 잘못 설치하면 설치에 성공할 수 있지만 이 문제는 잘못된 설치로 인해 발생한 것으로 간주됩니다. 증거에 따르면 시그니처 메타데이터가 센서 수준(GID:SID:REV로 식별된 이벤트)에 존재했지만 데이터베이스 손상으로 인해 적절한 메시지 표시 또는 syslog 내보내기를 위해 FMC에서 확인할 수 없었습니다.

관련 콘텐츠

- [Cisco 버그 ID CSCwu63768](#)
- [Sourcefire 규칙 업데이트 다운로드](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.