

Eventos de intrusão do FMC exibem "Alerta de Snort" genérico Mensagens

Contents

Problema

- Os eventos de invasão não exibem mais mensagens descritivas de regra do Snort na GUI do FMC e resultam na perda de informações de alerta acionáveis e afetam os recursos de monitoramento de segurança.
- Uma mensagem de evento de intrusão para respostas de eco normalmente mostra o seguinte:

- PROTOCOL-ICMP Echo Reply (1:408:8)

No entanto, o problema faz com que as mensagens de snort apareçam mais genericamente como "Snort Alert" (Alerta Snort):

Snort Alert (1:408:8)

- Os nomes de regra e descrições reais exibidos nos eventos são apenas entradas genéricas, como 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

- Na Visualização de pacotes, o mesmo tipo de mensagem aparece com Regra indisponível nas Informações do 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

- Além disso, os eventos de syslog exportados de sistemas FMC para SIEM contêm valores vazios para estes campos:
 - sig_id

- signature_msg
- descassinatura
- O registro de mensagens do FMC mostra erros repetidos em vários eventos de intrusão relacionados a mensagens de evento:

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

- O problema afeta todos os eventos de intrusão que chegam ao FMC dos sensores gerenciados e persiste nas atualizações normais da Sourcefire Rule Update (SRU) e do Local Security Package (LSP) do FMC.

Ambiente

- Visto pela primeira vez no Cisco Secure Firewall Management Center 2600 executando o FMC 7.2.11 (build 313) em alta disponibilidade (HA)
- As atualizações regulares de SRU/LSP, GeoDB e VDB estavam sendo aplicadas, mas não resolveram o problema

Resolução

O problema é resolvido com a execução de uma reinstalação forçada do pacote Sourcefire Rule Update (SRU) para recriar corretamente o banco de dados de mensagens de assinatura do Snort.

1.- Acesse o FMC CLI e verifique o pacote SRU instalado mais recente:

```
<#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.- Execute a reinstalação forçada do pacote 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.- Rastreie o progresso da instalação usando 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
```



Note: A instalação da SRU pode levar até 20 minutos para ser concluída e pode parecer que ela permanece em determinadas porcentagens por vários minutos. Este é um comportamento normal.

4: Após a conclusão bem-sucedida da reinstalação forçada do SRU:

- Monitorar novos eventos na página de eventos de intrusão do FMC
- Verifique se os novos eventos de intrusão exibem mensagens de regra de Snort adequadas em vez de entradas genéricas de "Alerta de Snort"
- Confirme se as exportações de syslog para sistemas SIEM agora contêm campos de assinatura preenchidos



Tip: Esta correção não é retroativa. Os eventos gerados anteriormente sem a mensagem apropriada permanecem inalterados, mas todos os novos eventos de intrusão devem exibir mensagens de regra de Snort corretas e preencher os campos de syslog corretamente.

Causa

Um defeito no FMC causou corrupção e/ou dessincronização do banco de dados de mensagens de assinatura do Snort, impedindo o FMC de resolver e preencher os metadados da regra do Snort em eventos de invasão. Esse comportamento é rastreado sob a ID de bug Cisco CSCwu63768.

Acredita-se que o problema seja disparado pela instalação incorreta de uma atualização SRU/LSP anterior, mesmo que a instalação possa ser bem-sucedida. Os elementos de prova mostraram que os metadados de assinatura existiam a nível do sensor (eventos identificados por GID:SID:REV), mas não puderam ser resolvidos pelo FMC para exibição adequada de mensagens ou exportação de syslog devido à corrupção do banco de dados.

Conteúdo relacionado

- [ID de bug Cisco CSCwu63768](#)
- [Downloads de atualização de regras do Sourcefire](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.