

FMC侵入イベントで一般的な"Snort Alert" ; メッセージが表示される

内容

問題

- 侵入イベントでは、FMC GUIに説明的なSnortルールメッセージが表示されなくなり、その結果、実用的なアラート情報が失われ、セキュリティモニタリング機能に影響を与えます。
- 通常、エコー応答の侵入イベントメッセージは次のように表示されます。
- PROTOCOL-ICMPエコー応答(1:408:8)

ただし、この問題により、Snortメッセージはより一般的に「Snort Alert」として表示されます。

Snort Alert (1:408:8)

- 実際に表示されるルール名と説明のイベントは、Snort Alert(gid:sid:"rev)などの一般的なエントリのみです。

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

- パケットビューでは、同じタイプのメッセージがEvent InformationにRule Unavailableと表示されます。

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

- さらに、FMCからSIEMシステムにエクスポートされるsyslogイベントには、次のフィールドに対して空の値が含まれます。
 - シグニチャID

- signature_msgの実行結果
- signature_descを実行する
- FMCメッセージログに、イベントメッセージに関する複数の侵入イベントの繰り返しエラーが表示されます。

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

- この問題は、管理対象センサーからFMCに送られるすべての侵入イベントに影響し、通常のFMC Sourcefire Rule Update(SRU)とLocal Security Package(LSP)のアップデートを行っても発生し続けます。

環境

- FMC 7.2.11 (ビルド313) をハイアベイラビリティ(HA)で実行するCisco Secure Firewall Management Center(FMC)2600で最初に表示
- 定期的なSRU/LSP、GeoDB、およびVDBの更新が適用されましたが、問題は解決しませんでした

解決方法

この問題は、Sourcefire Rule Update(SRU)パッケージの強制的な再インストールを実行して、Snortシングニチャメッセージデータベースを正しく再構築することで解決されます。

1.- FMC CLIにアクセスし、インストールされている最新のSRUパッケージを確認します。

```
<#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パッケージの強制的な再インストールを実行します。

<#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.- 次のコマンドを使用して、インストールの進行状況を追跡します。

<#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_iro_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
```



注:SRUのインストールは、完了までに最大で20分かかる場合があります、特定の割合で数分間持続するように見えます。これは正常な動作です。

4：強制SRU再インストールが正常に完了した後：

- FMC侵入イベントページで新しいイベントを監視します
- 新しい侵入イベントで、一般的な「Snort Alert」エントリではなく、適切なSnortルールメッセージが表示されることを確認します。
- SIEMシステムへのsyslogエクスポートにシグニチャフィールドが入力されていることを確認します。



ヒント：この修正は遡及的ではありません。適切なメッセージなしで以前に生成されたイベントは変更されませんが、新しい侵入イベントはすべて正しいSnortルールメッセージを表示し、syslogフィールドに適切に入力する必要があります。

原因

FMCの不具合により、Snortシグニチャメッセージデータベースの破損や非同期が発生し、FMCが侵入イベントでSnortルールメタデータを解決して入力することができなくなりました。この動作は、Cisco Bug ID CSCwu63768で追跡されています。

この問題は、以前のSRU/LSPアップデートの不適切なインストールによって引き起こされると考えられます。ただし、インストールは成功する可能性があります。シグニチャメタデータがセンサーレベル（GID:SID:REVで識別されるイベント）に存在するものの、データベース破損のため、メッセージの適切な表示やsyslogエクスポートのためにFMCで解決できないことを示す証拠があります。

関連コンテンツ

- [Cisco Bug ID CSCwu63768](#)
- [Sourcefireルール更新プログラムのダウンロード](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。