FTD升級期間，由於自訂原則檢測，Snort引擎升級受阻

目錄

問題

在由FMC管理的HA FPR-4115上，從7.2版升級到7.4.4版期間，Snort引擎升級到Snort 3會被阻止，並顯示錯誤消息，指出無法轉換Snort 2自定義規則或使用自定義入侵或網路分析策略。特定錯誤消息表明：無法升級到Snort 3。裝置至少使用一個自定義入侵策略或網路分析策略。 更詳細的故障消息引用無法轉換Snort 2自定義規則，並指向/var/sf/htdocs/ips/snort.rej瞭解詳細資訊。問題在於此錯誤是否會阻止遷移到Snort 3和影響檢測功能。

環境

- 思科安全防火牆Firepower版本7.3
- Firepower管理中心(FMC)版本7.7.11
- 高可用性(HA)配置中的FTD裝置
- 硬體：FPR-4115
- 升級路徑：FTD 7.2至7.4.4
- 升級前最新版本的VDB
- Objects > Intrusion Rules > Snort 2 All Rules下的Local Rules部分為空

解析

阻止Snort引擎升級的錯誤訊息是與Cisco錯誤ID CSCwn46794相關的已記錄行為，當不存在實際的自定義Snort 2規則時，該訊息並不表示功能阻止程式。

驗證步驟

第1步：驗證自定義Snort 2規則狀態

導覽至FMC介面並檢查自訂Snort 2規則：

```
Objects > Intrusion Rules > Snort 2 All Rules > Local Rules
```

第2步：確認VDB版本

繼續進行升級之前，請確保漏洞資料庫(VDB)是最新版本。

第3步：檢視錯誤詳細資訊

檢查被引用檔案中的詳細錯誤資訊：

```
/var/sf/htdocs/ips/snort.rej
```

升級程式

當「本地規則」部分被確認為空（不存在自定義Snort 2規則）時，儘管出現錯誤消息，仍可以繼續升級。在此方案中，阻塞錯誤是誤報，並不表示需要轉換的實際自定義規則。

第1步：繼續進行Snort 3升級

繼續FTD升級至7.4.4版（包括Snort 3引擎升級）的流程。

第2步：升級後驗證

升級成功完成後，使用Snort 3引擎測試流量以確認預期行為。

第3步：監控系統效能

驗證新Snort 3引擎的檢查功能是否按預期運行。

原因

升級阻止消息是與Cisco錯誤ID CSCwn46794關聯的有文檔記錄的行為。此錯誤導致系統顯示有關自定義入侵策略或網路分析策略的錯誤消息，即使不存在需要轉換的實際自定義Snort 2規則。當「本地規則」部分為空時，該錯誤消息顯示為誤報，但系統升級前驗證錯誤地標識了自定義策略的存在。

相關內容

- 思科錯誤ID CSCwn46794
- 思科錯誤ID CSCwk07199
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。