澄清FMC上的VDB更新過程

目錄

問題

當在漏洞資料庫(VDB)更新上運行時，管理員需要瞭解VDB更新是否為累積更新，以及是否可以跳過中間版本。

在本示例中，問題是從VDB版本393更新到版本427時的問題。具體來說，不確定是否需要多個升級步驟或是否支援直接升級路徑。此外，還擔心VDB更新及後續策略部署過程中可能會出現服務中斷。

環境

- Secure Firewall Management Center(FMC)軟體版本7.4.2.4。其他軟體版本也受到影響。
- FPR 2110上的防火牆威脅防禦(FTD)。其他硬體平台也受到影響。
- 當前VDB版本：393.其他軟體版本也受到影響。
- 目標VDB版本：427.其他軟體版本也受到影響。

解析

FMC上的VDB更新是累積性的，允許從較舊版本直接升級到較新版本，而無需中間步驟。

VDB更新過程

您可以直接從VDB版本393更新到VDB版本427，而無需任何中間VDB升級步驟。從VDB版本357開始，思科支援在FMC平台上安裝任何早於基準VDB的VDB版本。

要下載最新VDB版本，請導航至思科軟體下載中心，網址為 https://software.cisco.com/download/home/286332319/type/286321931/release/VDB

服務影響注意事項

主要風險不與FMC上的VDB安裝本身相關聯，而是與VDB更新後FTD上的第一個策略部署相關聯。在大多數情況下，VDB更新後的第一個部署會重新啟動Snort進程，這會暫時中斷流量檢查。

在此中斷期間：

- 流量可能丟棄或通過而不進行進一步檢查。
- 具體行為取決於FTD如何設定以在流程重新啟動期間處理流量。

最佳實踐建議：

- 在計畫的維護時段內計劃策略部署部分。
- 與網路操作協調，以最大程度地減少使用者影響。
- 在部署過程期間和之後監視系統狀態。

原因

- 從VDB 357開始，您可以安裝任何回到FMC的基線VDB的VDB更新。
- 安裝需要重新部署策略以啟用新的漏洞簽名，這將觸發受管FTD裝置上的Snort進程重新啟動。當載入新資料庫並重新初始化檢測引擎時，此重新啟動會短暫中斷流量檢測功能。

相關內容

- Cisco Secure Firewall Management Center管理指南 — 系統更新
- 思科安全防火牆管理中心裝置配置指南 — 部署
- 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）。