對顯示Impact=Unknown的FMC入侵事件進行故障排除

目錄

問題

部署新的防火牆管理中心(FMC)並升級到7.7.12版後，所有入侵事件都顯示「Impact=Unknown」（影響=未知），而不是預期影響值。這可以防止觸發適當的警報機制，因為警報配置需要影響欄位。

環境

- FMC 7.7.12版。其他軟體版本也可能會受到影響。
- 在防禦或檢測模式下的入侵策略。

解析

此問題的解決涉及驗證和配置發現策略範圍，以包括生成入侵事件的所有相關IP地址。

步驟1.確定受影響的IP地址

檢視顯示「Impact=Unknown」（影響=未知）的入侵事件並確定這些事件中涉及的特定IP地址。記錄這些IP地址，以便與當前發現策略配置進行比較。

步驟2.檢視當前發現策略配置

導航到FMC Policies > Network Discovery (較新版本為 Policies > Advanced > Network Discovery)，檢查當前的發現策略設定，以確定當前發現範圍內包含的IP地址範圍或子網。

步驟3.更新發現策略範圍

修改發現策略配置，使其包括發生入侵事件的所有IP地址。確保發現策略範圍包含您預期接收入侵事件的所有網段，並進行適當的影響評估。

步驟4.部署配置更改

將更新的發現策略配置部署到所有受管裝置，以確保更改在整個安全基礎架構中生效。

步驟5.檢驗影響欄位填充

監視新的入侵事件，以確認影響欄位當前已填充適當的值，而不是「未知」。

原因

顯示「Impact=Unknown」（影響=未知）的入侵事件是由配置問題引起的，在此配置問題中，受影響的IP地址未包含在FMC上的任何發現策略中。當IP地址超出配置的發現策略範圍時，FMC無法正確評估入侵事件對這些地址的影響，從而導致影響欄位填入「未知」值。這是一個與配置相關的問題，而不是軟體或硬體缺陷。

相關內容

- 入侵事件影響級別
- 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）。