思科安全終端覆蓋請求最佳實踐

目錄

簡介

本文檔介紹為已識別但安全終端當前未檢測到的已知威脅請求Talos覆蓋時必須使用的流程。

不同的資訊來源

識別和發佈這些威脅的來源可能有多種，以下是一些常用的平台：

- 已發佈Cisco CVE
- 已發佈的CVE（常見漏洞和洩露）
- Microsoft諮詢
- 第三方威脅情報

思科希望確保資料來源是合法的，然後再讓Talos檢視資訊並確定相關覆蓋範圍。

為了審查思科對相關威脅的立場和覆蓋範圍，我們有各種思科/Talos來源，在請求新的覆蓋範圍請求之前必須對其進行審查。

思科漏洞門戶

如需與思科產品相關的任何CVE，請參閱此入口網站，瞭解詳細資訊：https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Talos門戶

Talos情報門戶必須成為檢視此威脅是否已調查或當前由Talos調查的第一個參考點：https://talosintelligence.com/

Talos部落格

思科Talos部落格還提供有關Talos評估和調查的威脅的資訊：https://blog.talosintelligence.com/

我們能夠找到「Vulnerability Information」（漏洞資訊）下的大部分相關資訊，該資訊還包括所有已發佈的「Microsoft Advisories」（Microsoft諮詢）。

使用思科產品進行其他調查

思科提供多種產品，可幫助檢視威脅媒介/雜湊，並確定安全終端是否提供威脅覆蓋範圍。

Cisco SecureX思科威脅響應調查(CTR)

我們可以在CTR調查中調查威脅載體，更多資訊可以在此處檢視：https://docs.securex.security.cisco.com/Threat-Response-Help/Content/investigate.html

Cisco XDR調查

Cisco XDR提供用於調查威脅媒介的增強功能，有關功能的詳細資訊，請訪問以下網址:https://docs.xdr.security.cisco.com/Content/Investigate/investigate.htm

有用的思科部落格

請閱讀這些部落格，瞭解上一節中討論的一些功能：

https://blogs.cisco.com/tag/relevant-and-extended-detection-with-securex

後續步驟

如果沒有找到使用上述步驟涵蓋的威脅載體，我們可以通過提交TAC支援請求來請求威脅的Talos覆蓋範圍。

https://www.cisco.com/c/en/us/support/index.html

為了加快覆蓋請求的評估和調查，我們將請求以下有關威脅的資訊：

- 威脅情報的來源(CVE/Advisory/第三方調查/Technotes/Blogs)
- 關聯SHA256雜湊
- 檔案示例（如果可用）。

一旦獲得此資訊，Talos將相應稽核並調查請求。

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）。