修復安全終結點上顯示的漏洞

目錄

簡介

必要條件

- 需求
- 採用元件

問題

解決方案

簡介

本檔案介紹如何檢查終端思科風險評分及應用修正。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全終端主控台

採用元件

本檔案中的資訊是根據以下軟體版本：

- 安全終端控制檯5.4.2025030619

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

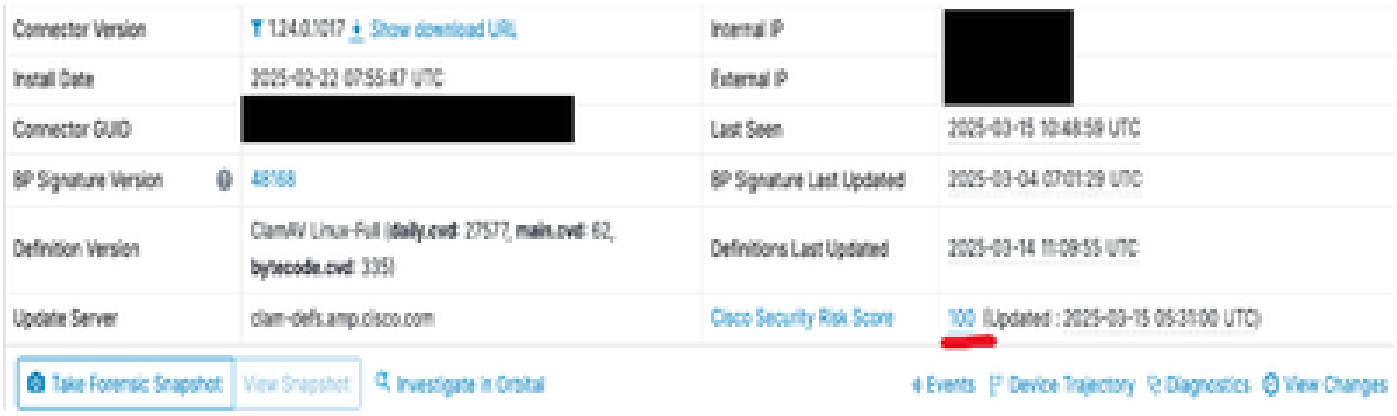
思科安全風險評分的等級從0到100。它通過檢視技術嚴重性和真實攻擊者如何利用此漏洞來量化漏洞風險。

檢查終端的Cisco安全風險評分並應用建議的修復程式。

解決方案

1 — 要檢視Cisco安全風險評分，請導航到Management > Computers並選擇Cisco Security Risk Score顯示：

2 — 您會看到電腦清單。展開要檢查的電腦資訊，然後按如下所示的Cisco Security Risk Score編號：



3 — 您會看到影響終端的CVE清單。按如下所示按一下Fix Available:

4 — 此處您會看到針對下面列出的CVE的建議修復：

Vulnerability Fixes

CVE-2023-4863

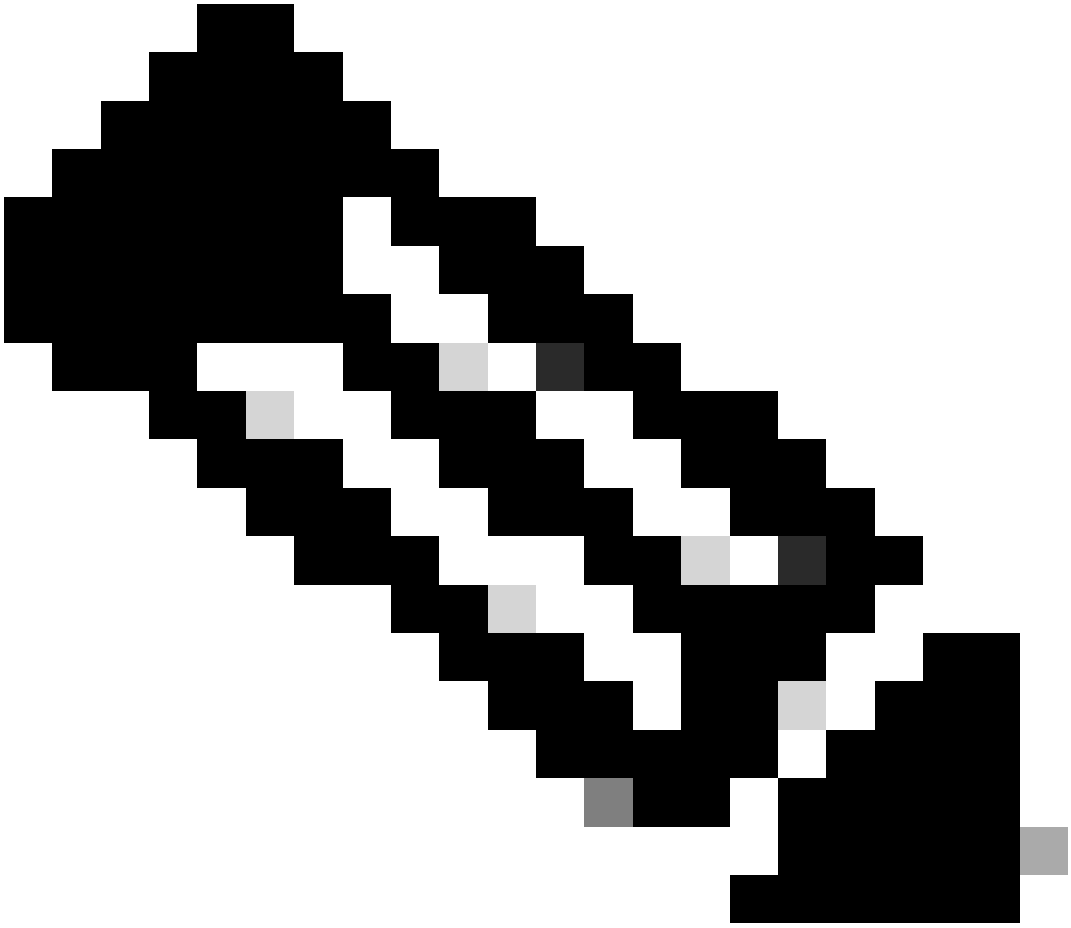
100 / 100
CVSS 3.1: 8.8

Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libwebp 1.3.2 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)

Fixed By:

- USN-6368-1

Close



附註：如果沒有可用的修復，請聯絡TAC。

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）。