張貼日期：2023/06/19

【資安漏洞預警Cisco ASA 和 Cisco FTD 在為 SSLTLS 配置的 Cisco Firepower 2100 系列設備上運行存在弱點，建議請管理者儘速評估更新！

- 主旨說明Cisco ASA 和 Cisco FTD 在為 SSLTLS 配置的 Cisco Firepower 2100 系列設備上運行存在弱點，建議請管理者儘速評估更新！
- 內容說明：
  - 轉發 中華資安國際 CHTSecurity-ANA-202306-0005
  - 思科自適應安全設備 (ASA) 軟體和適用於思科 Firepower 2100 系列設備的思科 Firepower 威脅防禦 (FTD) 軟體的基於硬體的 SSL/TLS 加密功能中的弱點可能允許未經身份驗證的遠端攻擊者導致受影響的設備重新載入，導致阻斷服務 (DoS) 情況。此弱點是由於 SSL/TLS 流量處理的加密函數在卸載到硬體時出現了實現錯誤。
  - 攻擊者可以通過向受影響的設備發送精心製作的 SSL/TLS 流量流來利用此弱點。成功的利用可能允許攻擊者在基於硬體的加密引擎中造成意外錯誤，這可能導致設備重新加載。
- 影響平台:
  - Cisco ASA 9.16.4 版本
  - Cisco ASA 9.18.2 版本
  - Cisco ASA 9.18.2.5 版本
  - Cisco FTD 7.2.1 版本
  - Cisco FTD 7.2.1 版本
  - Cisco FTD 7.2.3版本
- 建議措施:
  - 請參考 Cisco 官方更新版本或安裝修補更新：

https://sec.cloudapps.cisco.com/security/center/publicationListing.x

- 參考資料:
  1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ssl-dos-uu7mV5p6
  2. https://sec.cloudapps.cisco.com/security/center/publicationListing.x

---

計算機與通訊中心
網路系統組 敬啟