調查 TLS填充FTD上的Oracle漏洞(CVE-2019-1559)

目錄

問題

- 在滲透測試期間，在思科防火牆威脅防禦(FTD)裝置上報告了一個標識為CVE-2019-1559的TLS填充Oracle漏洞（殭屍POODLE和GOLDENDOODLE）。
- 在與FTD介面關聯的IP位址上偵測到漏洞。
- 漏洞報告對潛在的安全風險表示擔憂，需要進行調查和補救。

環境

- 硬體：任意
- SW:Cisco安全FTD版本7.4.2.4。也可報告其他軟體版本。

解析

- 對運行7.4.2.4版的FTD裝置所報告的漏洞CVE-2019-1559（TLS Padding Oracle漏洞 — Zombie POODLE和GOLDENDOODLE）進行了徹底調查。漏洞掃描程式已生成假陽性結果，所報告的裝置未受CVE-2019-1559的影響。
- 由於FTD 7.4.2.4版不易受報告的TLS Padding Oracle漏洞的影響，因此無需採取進一步操作來解決此安全問題。
- 有關其他資訊，請檢視https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve

原因

漏洞報告由確定潛在接觸CVE-2019-1559的滲透測試工具生成。但是，已確定FTD 7.4.2.4版不受此特定TLS Padding Oracle漏洞的影響。警報的原因可能是漏洞掃描工具提供的誤報或此裝置對此特定CVE敏感性的評估不正確。

相關內容

- https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve
- 思科錯誤ID CSCvp80474
- https://www.cve.org/CVERecord?id=CVE-2019-1559
- https://nvd.nist.gov/vuln/detail/cve-2019-1559

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）。