

Investigate TLS Padding Oracle Vulnerability (CVE-2019-1559) auf FTD

Inhalt

Problem

- Während des Penetrationstests wurde eine TLS Padding Oracle Vulnerability (Zombie POODLE und GOLDENDOODLE), die als CVE-2019-1559 identifiziert wurde, auf einem Cisco Firewall Threat Defense (FTD)-Gerät gemeldet.
- Die Schwachstelle wurde an einer IP-Adresse entdeckt, die mit einer FTD-Schnittstelle verknüpft ist.
- Im Schwachstellenbericht wurden Bedenken hinsichtlich eines potenziellen Sicherheitsrisikos laut, das untersucht und behoben werden muss.

Umwelt

- HW: Beliebig
- SW: Cisco Secure FTD Version 7.4.2.4. Andere Softwareversionen können ebenfalls gemeldet werden.

Auflösung

- Die gemeldete Schwachstelle CVE-2019-1559 (TLS Padding Oracle Vulnerability - Zombie POODLE und GOLDENDOODLE) wurde für das FTD-Gerät mit Version 7.4.2.4 gründlich untersucht. Der Schwachstellen-Scanner hat ein falsch positives Ergebnis ergeben und das gemeldete Gerät ist nicht betroffen von CVE-2019-1559
- Es waren keine weiteren Maßnahmen erforderlich, um diese Sicherheitsbedenken auszuräumen, da die FTD-Version 7.4.2.4 nicht anfällig für die gemeldete TLS Padding

Oracle-Schwachstelle ist.

- Weitere Informationen finden Sie unter <https://sec.cloudapps.cisco.com/security/center/cvr?cveldList=CVE-2019-1559#~cve>

Ursache

Der Schwachstellenbericht wurde von Tools für Penetrationstests erstellt, die eine potenzielle Gefährdung durch CVE-2019-1559 identifizierten. Es wurde jedoch festgestellt, dass FTD Version 7.4.2.4 von dieser spezifischen TLS Padding Oracle Schwachstelle nicht betroffen ist. Die Ursache der Warnung war wahrscheinlich ein falscher positiver Befund des Vulnerability Scanning Tools oder eine falsche Einschätzung der Anfälligkeit dieses Geräts für diesen speziellen CVE.

Verwandte Inhalte

- <https://sec.cloudapps.cisco.com/security/center/cvr?cveldList=CVE-2019-1559#~cve>
- Cisco Bug-ID [CSCvp80474](#)
- <https://www.cve.org/CVERecord?id=CVE-2019-1559>
- <https://nvd.nist.gov/vuln/detail/cve-2019-1559>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.