Analizza TLS Padding Oracle Vulnerability (CVE-2019-1559) su FTD

Sommario

Problema

- Durante i test di penetrazione, un TLS Padding Oracle Vulnerability (Zombie POODLE e GOLDENDOODLE) identificato come CVE-2019-1559 è stato segnalato su un dispositivo Cisco Firewall Threat Defense (FTD).
- È stata rilevata la vulnerabilità su un indirizzo IP associato a un'interfaccia FTD.
- La relazione sulla vulnerabilità ha sollevato preoccupazioni in merito a potenziali rischi per la sicurezza che richiedono indagini e misure correttive.

Ambiente

- HARDWARE: Qualsiasi
- Software: Cisco Secure FTD versione 7.4.2.4. È possibile segnalare anche altre versioni software.

Risoluzione

- La vulnerabilità segnalata CVE-2019-1559 (TLS Padding Oracle Vulnerability - Zombie POODLE e GOLDENDOODLE) è stata attentamente studiata per il dispositivo FTD in esecuzione versione 7.4.2.4. Lo scanner di vulnerabilità ha prodotto un risultato falso positivo e il dispositivo segnalato non è influenzato da CVE-2019-1559.
- Non sono state necessarie ulteriori azioni per risolvere questo problema di sicurezza, poiché la versione 7.4.2.4 del FTD non è soggetta alla vulnerabilità di TLS Padding Oracle segnalata.

- Per ulteriori informazioni, visitare il sito https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve

Causa

Il rapporto sulla vulnerabilità è stato generato da strumenti di test di penetrazione che hanno identificato una potenziale esposizione al CVE-2019-1559. Tuttavia, è stato determinato che FTD versione 7.4.2.4 non è influenzato da questa vulnerabilità specifica di TLS Padding Oracle. La causa dell'avviso è stata probabilmente un falso positivo proveniente dallo strumento di analisi della vulnerabilità o una valutazione errata della suscettibilità di questo dispositivo a questo particolare CVE.

Contenuto correlato

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).