Enquêter Vulnérabilité Oracle de remplissage TLS (CVE-2019-1559) sur FTD

Table des matières

Problème

- Lors des tests de pénétration, une vulnérabilité Oracle de remplissage TLS (Zombie POODLE et GOLDENDOODLE) identifiée comme CVE-2019-1559 a été signalée sur un périphérique Cisco Firewall Threat Defense (FTD).
- La vulnérabilité a été détectée sur une adresse IP associée à une interface FTD.
- Le rapport de vulnérabilité a soulevé des préoccupations concernant une exposition potentielle à la sécurité nécessitant une enquête et une correction.

Environnement

- MATÉRIEL : tous les modèles
- Logiciel : Cisco Secure FTD version 7.4.2.4. D’autres versions logicielles peuvent également être signalées.

Résolution

- La vulnérabilité signalée CVE-2019-1559 (TLS Padding Oracle Vulnerability - Zombie POODLE et GOLDENDOODLE) a fait l’objet d’une enquête approfondie pour le périphérique FTD exécutant la version 7.4.2.4. L’analyseur de vulnérabilité a produit un résultat faussement positif et le périphérique signalé n’est pas affecté par CVE-2019-1559.
- Aucune autre action n'était nécessaire pour résoudre ce problème de sécurité, car la version FTD 7.4.2.4 n'est pas sensible à la vulnérabilité Oracle TLS Padding signalée.

- Pour plus d'informations, consultez le site https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve

Motif

Le rapport de vulnérabilité a été généré par des outils de test de pénétration qui ont identifié une exposition potentielle au CVE-2019-1559. Cependant, il a été déterminé que la version FTD 7.4.2.4 n'est pas affectée par cette vulnérabilité spécifique de TLS Padding Oracle. La cause de l'alerte était probablement un faux positif de l'outil d'analyse de vulnérabilité ou une évaluation incorrecte de la susceptibilité de ce périphérique à ce CVE particulier.

Autres informations utiles

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.