Investigar Vulnerabilidad de Oracle de relleno de TLS (CVE-2019-1559) en FTD

Contenido

Problema

- Durante las pruebas de penetración, se notificó una vulnerabilidad de Oracle de relleno de TLS (Zombie POODLE y GOLDENDOODLE) identificada como CVE-2019-1559 en un dispositivo Cisco Firewall Threat Defense (FTD).
- La vulnerabilidad se detectó en una dirección IP asociada a una interfaz FTD.
- El informe de vulnerabilidad planteaba preocupación por la posible exposición de la seguridad que requería investigación y remediación.

Entorno

- HW: cualquiera
- SW: Cisco Secure FTD versión 7.4.2.4. También se pueden notificar otras versiones de software.

Resolución

- La vulnerabilidad notificada CVE-2019-1559 (vulnerabilidad de Oracle de relleno de TLS - Zombie POODLE y GOLDENDOODLE) se investigó exhaustivamente para el dispositivo FTD que ejecuta la versión 7.4.2.4. El analizador de vulnerabilidades ha producido un resultado falso positivo y el dispositivo notificado no se ve afectado por CVE-2019-1559.
- No fue necesario realizar ninguna otra acción para solucionar este problema de seguridad, ya que la versión 7.4.2.4 del FTD no es susceptible a la vulnerabilidad de Oracle de relleno de TLS notificada.

- Para obtener más información, visite https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve

Causa

El informe de vulnerabilidad se generó mediante herramientas de pruebas de penetración que identificaron la exposición potencial a CVE-2019-1559. Sin embargo, se determinó que la versión 7.4.2.4 de FTD no se ve afectada por esta vulnerabilidad específica de Oracle de relleno de TLS. La causa de la alerta fue probablemente un falso positivo de la herramienta de análisis de vulnerabilidades o una evaluación incorrecta de la susceptibilidad de este dispositivo a este CVE concreto.

Contenido relacionado

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).