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

Contents

Issue

- During penetration testing, a TLS Padding Oracle Vulnerability (Zombie POODLE and GOLDENDOODLE) identified as CVE-2019-1559 was reported on a Cisco Firewall Threat Defense (FTD) device.
- The vulnerability was detected on an IP address associated with the an FTD interface.
- The vulnerability report raised concerns about potential security exposure requiring investigation and remediation.

Environment

- HW: Any
- SW: Cisco Secure FTD version 7.4.2.4. Other software versions can be also reported.

Resolution

- The reported vulnerability CVE-2019-1559 (TLS Padding Oracle Vulnerability - Zombie POODLE and GOLDENDOODLE) was thoroughly investigated for the FTD device running version 7.4.2.4. The vulnerability scanner has produced a false positive result and the reported device is not impacted by CVE-2019-1559.
- No further action was necessary to address this security concern, as the FTD version 7.4.2.4 is not susceptible to the reported TLS Padding Oracle vulnerability.
- For additional information, check https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve

Cause

The vulnerability report was generated by penetration testing tools that identified potential exposure to CVE-2019-1559. However, it was determined that FTD version 7.4.2.4 is not affected by this specific TLS Padding Oracle vulnerability. The cause of the alert was likely a false positive from the vulnerability scanning tool or an incorrect assessment of the susceptibility of this device to this particular CVE.

Related Content

- https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=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