调查 TLS填充FTD上的Oracle漏洞(CVE-2019-1559)

目录

问题

- 在渗透测试期间，在思科防火墙威胁防御(FTD)设备上报告了一个标识为CVE-2019-1559的TLS填充Oracle漏洞（僵尸POODLE和GOLDENDOODLE）。
- 在与FTD接口关联的IP地址上检测到漏洞。
- 漏洞报告对潜在的安全风险表示担忧，需要进行调查和补救。

环境

- 硬件：any
- 软件：Cisco Secure FTD版本7.4.2.4。也可以报告其他软件版本。

分辨率

- 对运行版本7.4.2.4的FTD设备所报告的漏洞CVE-2019-1559（TLS填充Oracle漏洞 — Zombie POODLE和GOLDENDOODLE）进行了彻底调查。漏洞扫描程序生成了误报结果，所报告的设备未受到CVE-2019-1559的影响。
- 由于FTD版本7.4.2.4不易受报告的TLS Padding Oracle漏洞的影响，因此无需采取进一步操作来解决此安全问题。
- 有关更多信息，请访[问https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve](https://sec.cloudapps.cisco.com/security/center/cvr?cveIdList=CVE-2019-1559#~cve)

原因

漏洞报告由确定潜在接触CVE-2019-1559的渗透测试工具生成。但是，已确定FTD 7.4.2.4版不受此特定TLS Padding Oracle漏洞的影响。警报的原因可能是漏洞扫描工具提供的误报或此设备对此特定CVE敏感性的评估不正确。

相关内容

- 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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。