2017 年 5 月 8 日，星期一

漏洞聚焦：WolfSSL 库 X.509 证书文本解析代码执行漏洞

漏洞发现者：思科 Talos 团队的 Aleksandar Nikolic

简介

Talos 披露了在 WolfSSL 中发现的 TALOS-2017-0293/CVE 2017-2800 代码执行漏洞。WolfSSL 是一个轻量级 SSL/TLS 库，由于其尺寸小且性能高，因此专用于嵌入式和 RTOS（实时操作系统）环境。WolfSSL 广泛用于 ICS 和物联网设备等各种产品中。

该漏洞与使用 x.509 证书和处理 DER 证书中字符串字段的代码有关，特别是负责解析 "commonName"、"countryName"、"localityName"、"stateName"、"orgName"和 "orgUnit" 的代码。经特殊设计的 x.509 证书可能导致单个越界覆盖，引起证书验证问题、拒绝服务或远程代码执行。要触发该漏洞，攻击者需要向利用此库的服务器或客户端应用提供恶意的 x.509 证书。有关该漏洞的完整详细信息，请点击此处。

防护

以下 Snort 规则将检测相关的漏洞攻击尝试。请注意，Talos 未来可能会发布更多规则，当前的规则可能会根据可能得到的更多漏洞信息而有所变更。如需获取有关最新规则的信息，请参阅防御中心或 Snort.org。

Snort 规则：42000

发布者：NICK BIASINI；发布时间：12:54
标签：零日、TALOS、漏洞研究、漏洞聚焦