ACG1000是否涉及TLS 版本 1.0 协议检测漏洞

漏洞相关 王奎银 2022-02-23 发表

漏洞相关信息

漏洞编号： 无
漏洞名称： TLS 版本 1.0 协议检测
产品型号及版本： ACG1000系列

漏洞描述

远程服务接受使用 TLS 1.0 加密的连接。TLS 1.0 有许多加密设计缺陷。TLS 1.0的现代实现缓解了这些问题，但较新版本的TLS（如1.2和1.3）是针对这些缺陷而设计的，应尽可能使用。自 2020 年 3 月 31 日起，为 TLS 1.2 及更高版本启用了鈥樋的端点将不再在 major Web 浏览器和主要供应商中正常运行。PCI DSS v3.2 要求在 2018 年 6 月 30 日之前完全禁用 TLS 1.0，但 POS POI 终端（以及它们所连接的 SSL/TLS 终止点）除外，这些终端可以验证为不容易受到任何已知 exploit 的影响。

漏洞解决方案

版本R6611以后的443管理是屏蔽了TLS1.0, 启用对 TLS 1.2 和 1.3 的支持。