服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)

漏洞 聂骋 2021-06-18 发表

漏洞相关信息

漏洞编号： CVE-2011-1473

漏洞名称： 服务器支持 TLS Client-initiated 重协商攻击

产品型号及版本： F5000-M

漏洞描述

由于服务器端的重新密钥协商的开销是客户端的15倍，则攻击者可利用这个过程向服务器发起拒绝服务攻击。OpenSSL 1.0.2及以前版本受影响

漏洞解决方案

升级R9616P39或R9628P2412或更新