关于中低端与高端安全产品是否涉及CVE-2022-0778漏洞

漏洞相关 孔德飞 2023-08-14 发表

漏洞相关信息

漏洞编号： CVE-2022-0778

漏洞名称： OpenSSL拒绝服务漏洞通告

产品型号及版本： 中低端安全产品与高端产品

漏洞描述

该漏洞是由于OpenSSL库中BN_mod_sqrt()函数存在一个错误，导致其在非质数的情况下无限循环。当解析包含压缩形式的椭圆曲线公钥或者带有显式椭圆曲线参数的证书时，会使用到BN_mod_sqrt()函数。攻击者可以通过构造具有无效显式曲线参数的证书来触发无限循环操作，由于证书解析发生在证书签名验证之前，因此任何解析外部提供的证书的过程都可能受到拒绝服务攻击。

漏洞解决方案

中低端安全设备

B64D060SP23之前的版本即D060SP23之前的涉及，B64D060SP23以及之后的版本不涉及

高端产品如下

B64D045SP37之前的版本即D045SP37之前的版本涉及， B64D045SP37及以后版本修复即D045SP37之后的版本修复