V7防火墙系列产品是否涉及漏洞（CVE-2020-1971）

漏洞扫描 王奎银 2020-12-16 发表

问题描述

关于OpenSSL拒绝服务漏洞的紧急通报

一、漏洞情况

2020年12月8日，OpenSSL发布安全通告公布了一个空指针解引漏洞（CVE-2020-1971），官方评级高危。该漏洞存在于OpenSSL的函数GENERAL_NAME_cmp中，GENERAL_NAME_cmp函数可用来比较GENERAL_NAME的不同实例，以查看它们是否相等。当被比较的两个GENERAL_NAME都包含EDIPartyName时，将触发空指针解引用，造成程序崩溃最终导致拒绝服务。

二、影响版本

OpenSSL 1.1.1

OpenSSL 1.0.2（已不再受公开支持）

三、漏洞修改建议

官方已经发布修复了漏洞的新版本，详细信息如下：https://www.openssl.org/source/

鉴于该漏洞影响范围较大，潜在危害程度较高，请各单位及时核查OpenSSL使用情况，修补漏洞，消除安全隐患。

解决方法

M9000/T9000/F5000/F1000系列防火墙等如果使用证书会涉及这个漏洞。

修复措施：使用pki证书时，在pki domain 下关闭crl检查；不使用PKI证书，不涉及该漏洞。