

#### 漏洞相关信息

漏洞编号: CVE-2021-3711、CVE-2021-3712

漏洞名称: OpenSSL缓冲区溢出漏洞

产品型号及版本: SNA Center E1209、SeerEngine-WAN E6105H06、SeerAnalyzer E2101P10、License Server E1150

#### 漏洞描述

漏洞描述:

(1) CVE-2021-3711

该漏洞是由于OpenSSL调用用来解密SM2加密的数据所用的API函数EVP\_PKEY\_decrypt时, 计算缓冲区大小存在错误, 攻击者可利用该漏洞, 构造恶意数据执行远程代码执行攻击, 最终可控制程序的运行或造成程序崩溃。

(2) CVE-2021-3712

该漏洞是由于OpenSSL用于存储ASN.1字符串的结构ASN1\_STRING在创建时没有严格遵守字符串的零字节结尾, 打印时可能发生读取缓冲区溢出, 攻击者可利用该漏洞, 构造恶意数据执行信息泄露攻击, 最终可造成服务器敏感性信息泄露或程序崩溃。

影响范围:

1.1.1<=OpenSSL<=1.1.1k

## 漏洞解决方案

SNA Center、SeerEngine-WAN、SeerAnalyzer、License Server产品不涉及OpenSSL缓冲区溢出漏洞。

