



CAS&CloudOS是否涉及CVE-2021-3449

邓翠萍 2021-04-27 发表

漏洞相关信息

漏洞编号： CVE-2021-3449

漏洞名称： Open SSL拒绝服务高危漏洞

产品型号及版本： CAS/CloudOS不涉及

漏洞描述

关于OpenSSL存在高危漏洞的预警通报

近期，监测发现OpenSSL存在拒绝服务高危漏洞，漏洞编号为CVE-2021-3449，受影响的版本为OpenSSL 1.1.1-1.1.1j。在OpenSSL TLS服务器启用TLSv1.2和重新协商功能情况下，攻击者可从客户端发送恶意构造ClientHello请求触发该漏洞，从而导致服务器拒绝服务。鉴于该漏洞影响范围大，潜在危害性高，请各单位务必重视，及时通报预警，组织本单位、本行业、本辖区开展隐患排查，受影响用户要尽快将OpenSSL升级至安全版本OpenSSL 1.1.1k (<https://openssl.org/>)。同时，要落实安全防护措施，提升安全防护能力，完善事件应急处置预案，加强安全监测和值班值守。发现网络攻击情况要第一时间启动应急处置预案并及时报告我中心和属地公安机关。

漏洞解决方案

CAS和CloudOS均不涉及该漏洞。

【验证方法】：

可以在服务器后台执行openssl version命令查询产品使用的OpenSSL组件版本，由于漏洞CVE-2021-3449受影响的版本范围为OpenSSL 1.1.1-1.1.1j，如果不在上述范围内即是不涉及该漏洞。

```
[root@cloudos501 ~]# openssl version
```

OpenSSL 1.0.2k-fips 26 Jan 2017

```
[root@cvknode04 ~]# openssl version
```

OpenSSL 1.0.2k-fips 26 Jan 2017

