安全漏洞通告

OpenSSL 拒绝服务、证书绕过漏洞通告

360CERT

360CERT
北京奇虎科技有限公司 | 2021-03-26

报告信息

报告名称	OpenSSL 拒绝服务、证书绕过漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2021-032601
报告版本	1	**报告日期**	2021-03-26
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-03-26	360CERT	360CERT	撰写报告

360CERT

目录

360CERT

一、 漏洞档案

漏洞类型	证书校验
CVE 编号	CVE-2021-3450 等
相关厂商	openssl
相关组件	暂无
威胁等级	高危
影响面	广泛
360CERT 评分	8.8
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2021-03-26
报告生成时间	2021-03-26

360CERT

二、 漏洞简述

2021 年 03 月 26 日，360CERT 监测发现 OpenSSL 发布了 OpenSSL 的安全更新风险通告，漏洞编号为 CVE-2021-3450,CVE-2021-3449 ，漏洞等级：高危，漏洞评分：8.8。

OpenSSL 是一个开放源代码的软件库包，应用程序可以使用这个包来进行安全通信，同时确认连接者身份。这个包广泛被应用在互联网的网页服务器上。 例如： cisco 设备，apache server，nginx server 等。

对此，360CERT 建议广大用户及时将 OpenSSL 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

360CERT

三、 漏洞评级

经过安全技术人员的分析，最终对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	广泛
360CERT 评分	8.8

360CERT

四、 漏洞详情

CVE-2021-3450: 证书校验漏洞

CVE: CVE-2021-3450

组件: openssl

漏洞类型: 证书校验

影响: 通信、流量劫持

简述: 在开启 X509_V_FLAG_X509_STRICT 选项的 openssl 服务器上，由于 OpenSSL 对 X.509 证书链的验证逻辑中存在问题，导致受影响的系统接受由非 CA 证书或证书链签名的有效证书。攻击者可以通过使用任何有效的证书或证书链来签名精心制作的证书来利用此漏洞。成功的利用可能使攻击者能够进行中间人（MiTM）攻击并获取敏感信息(例如：访问受证书身份验证保护的网络或资产，窃听加密通信内容)。

CVE-2021-3449: 拒绝服务漏洞

CVE: CVE-2021-3449

组件: openssl

漏洞类型: 拒绝服务

影响: 服务宕机

简述: OpenSSL TLSv1.2 重新协商选项（默认开启）中存在一处空指针解引用，并导致拒绝服务

五、 漏洞列表

编号	描述	导致结果	威胁等级
CVE-2021-3450	证书校验	通信、流量劫持	高危
CVE-2021-3449	拒绝服务	服务宕机	高危

360CERT

六、 安全建议

(一) 通用修补方案

升级到 openssl 1.1.1k

(二) 临时修补方案

针对 CVE-2021-3449 漏洞可以通过如下方式进行自我检测。

openssl s_client -tls1_2 -connect your_domain:443

[按下 R 键]

查看关键词 RENEGOTIATING 下方是否有包含 verify 关键词的内容。若存在则受到影响

若出现 write:errno=0 则标识不受到该漏洞影响

360CERT

七、 产品侧解决方案

(一) 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台(quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或(quake#360.cn)获取对应产品。

360CERT

八、 参考链接

1. OpenSSL Vulnerabilities

   https://www.openssl.org/news/vulnerabilities.html

360CERT

附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

360CERT

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

360CERT

附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

360CERT

附录 C 360 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 – 10.0	严重
7.0 – 8.9	高危
4.0 – 6.9	中危
0 - 3.9	低危

360CERT