2021年11月8日

安全热点周报

第二百一十九期

本周安全大事件

Linux Kernel TIPC 远程代码执行漏洞安全风险通告：

2021 年 11 月 4 日，SentinelLabs的研究人员在 Linux Kernel 的TIPC模块中发现了一个堆溢出漏洞（CVE-2021-43267），该漏洞的 CVSS 评分为 9.8。该漏洞存在于 Linux Kernel 中的 net/tipc/crypto.c 中，远程攻击者可以通过 TIPC 功能以利用用户提供的 MSG_CRYPTO 消息类型大小验证不足来进行攻击。此外，TIPC模块随所有主要Linux发行版一起提供，但需要用户加载才能启用该协议（非系统自动加载）。攻击者可以远程或本地利用此漏洞以执行任意代码，获取内核权限，从而攻击整个系统。目前此漏洞补丁已发布，建议用户将 Linux kernel 更新到最新 5.15 版本。

本周漏洞热度排行

在本周热度舆论排行榜前五的漏洞中，热度最高的漏洞为 Git LFS 命令注入漏洞（CVE-2020-27955），该漏洞是由于 Git LFS 通过 exec.Command 函数执行新的 git 进程时，没有指定 git 二进制文件的完整路径。由于 Windows 系统上的 exec.Command 实现包括当前目录，因此攻击者可能只需添加名为 git.bat、git.exe、git.cmd 或任何其他文件的可执行文件，即可在恶意存储库中植入后门程序。攻击者可通过诱骗受害者克隆攻击者的恶意存储库来利用此漏洞，成功利用此漏洞可允许攻击者执行任意代码。

本周重要漏洞

漏洞编号	影响产品	危险等级	漏洞类型
CVE-2021-43267	Linux kernel	中危	任意代码执行
CVE-2021-30821	macOS Monterey	高危	任意代码执行
CVE-2021-42574	Unicode	中危	任意代码执行

注：以上漏洞为奇安信CERT研判后较为重要，但未达到风险通告标准的漏洞，可登录NOX安全监测平台（https://nox.qianxin.com）查看漏洞详细信息。

安全事件

① 伪装成防病毒应用的新型 Android 恶意软件正在日本传播

据 bleepingcomputer 网站报道，上周，日本安全研究人员发现了一个名为 FakeCop 的新变种 Android 信息窃取软件，正在通过带有恶意链接的短信和网络钓鱼电子邮件两种渠道快速传播。研究人员表示，该软件会伪装成日本流行的防病毒软件 Anshin Security 收集用户手机上的短信、联系人、账号信息、应用列表，修改或删除用户设备数据库中的短信，并在用户不知情的情况下发送短信。安全研究人员建议用户应避免点击未经确认的短信和电子邮件中的链接，避免安装官方商店之外的 APK 文件，并在安装新应用时仔细检查权限请求。

② Quickfox VPN 泄露 100 万用户数据

Quickfox 是一个免费虚拟私人网络（VPN）服务商，它提供了免费从国外访问中国网站的服务。近日，安全研究人员发现，由于 Quickfox 错误配置了 VPN 服务 Elasticsearch、Logstash 和 Kibana 的安全措施，导致任何人都可以使用浏览器和互联网来访问 Quickfox 的日志，并提取用户的敏感信息。目前已有超过一百万用户的 5 亿条记录和 100GB 的数据被泄露。被泄露的数据主要是电子邮件和电话号码等 PII，同时也有大约 30 万名 Quickfox 用户设备上的软件信息。这一事故让很多安全从业者对 VPN 的安全性产生了巨大的质疑，认为 VPN 作为通往内部网络的大门却一次又一次曝出安全漏洞，需要考虑是否弃用。