2021年12月6日

安全热点周报

第二百二十三期

223

本周安全大事件

泛微 E-Office 文件上传漏洞安全风险通告第二次更新：

泛微 e-office 是一款标准化的协同 OA 办公软件，实行通用化产品设计，充分贴合企业管理需求，本着简洁易用、高效智能的原则，为企业快速打造移动化、无纸化、数字化的办公平台。近日，奇安信CERT监测到泛微 E-Office 文件上传漏洞 (CNVD-2021-49104) 存在在野利用。由于泛微E-Office未能正确处理上传模块中输入的数据，未授权的攻击者可以构造恶意数据包发送给服务器，实现任意文件上传，并且获得服务器的 webshell，成功利用该漏洞可以获取服务器控制权，目前已监测到该漏洞存在在野利用。鉴于漏洞危害较大，利用无需权限，建议用户及时升级补丁。

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 Linux kernel TIPC 模块任意代码执行漏洞 (CVE-2021-43267)，该漏洞是由于 5.14.16 之前的 Linux 内核中的 net/tipc/crypto.c 存在一个问题，透明进程间通信 (TIPC) 功能允许远程攻击者利用用户提供的 MSG_CRYPTO 消息类型大小验证不足，攻击者可以构建一个 n 字节的数据包并将消息大小设置为小于 n 的长度，造成堆溢出。攻击者可以利用该漏洞任意代码执行。

本周重要漏洞

漏洞编号	影响产品	危险等级	漏洞类型
CVE-2021-43527	NSS	高危	堆溢出
CVE-2021-39237	FutureSmart	低危	信息泄露
CVE-2021-39238	FutureSmart	高危	远程代码执行
CVE-2021-30535	Chrome	中危	内存损坏

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 松下遭网络攻击，致数据泄露

日本跨国企业集团松下在本月遭遇不明黑客的网络攻击，攻击黑客获得其网络服务器访问权限后披露了安全漏洞，导致部分企业数据惨遭泄露。公开信息显示，松下于 11 月 11 日遭第三方非法入侵，不明身份的黑客访问了松下文件服务器上的一些数据。随后，松下将网络攻击事件上报有关当局，并及时采取措施防止其他外部服务器访问其网络系统。目前，松下已聘请第三方安全服务公司来调查此次攻击，后续将进一步查明不法攻击者入侵期间访问数据是否包含客户个人信息。

② 黑客使用“Babadeda Crypter”躲避杀软检测

近日，有安全团队发现一新型恶意软件活动，其通过 Discord 渠道针对加密货币、非同质代币（NFT）和 DeFi 爱好者部署了一个名为“Babadeda Crypter”的加密器，以此绕过杀毒软件进行攻击活动。据悉，该恶意软件分发活动最早始于 2021 年 5 月，Babadeda Crypter 是网络犯罪分子使用的一种软件，可以加密、混淆和操纵恶意代码，使其看起来似乎无害且难以被杀软检测到。幕后黑客还会在区块链相关的 Discord 频道上发送诱饵消息，诱导不明用户中招。

Copyright ©2021 奇安信CERT. All Rights Reserved.