2021年11月22日

安全热点周报

第二百二十一期

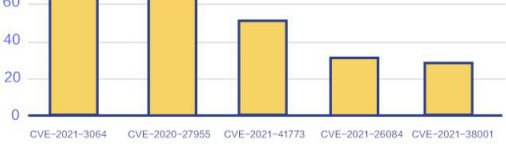
221

本周安全大事件

Apache Druid 任意文件读取漏洞安全风险通告：

近日，奇安信 CERT 监测到 Apache Druid任意文件读取漏洞细节及 EXP 在互联网公开，攻击者可通过将文件 URL 传递给 HTTP Input-Source来绕过应用程序级别的限制。由于 Apache Druid默认情况下缺乏授权认证，攻击者可构造恶意请求，在未授权情况下利用该漏洞读取任意文件，最终导致服务器敏感信息泄露。目前，Apache 官方已发布可更新版本，建议客户尽快自查修复。

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 Palo Alto Networks GlobalProtect 门户和网关接口远程代码执行漏洞（CVE-2021-3064），该漏洞是由于 GlobalProtect 不恰当地处理用户输入导致的缓冲区溢出，仅影响启用了 GlobalProtect 门户和网关的 PAN 防火墙。未经身份验证的远程攻击者通过发送特制请求并结合 HTTP 走私来利用此漏洞，成功利用此漏洞可在目标设备上以 ROOT 权限执行任意代码。

本周重要漏洞

漏洞编号	影响产品	危险等级	漏洞类型
暂无	Hadoop Yarn	高危	未授权访问
CVE-2021-0146	Intel	高危	特权提升
CVE-2021-41653	TL-WR840N	高危	远程代码执行
CVE-2021-41349	Microsoft Exchange Server	高危	信息泄露

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 macOS 曝出零日漏洞，不法分子借此发起水坑攻击

据谷歌 TAG 研究人员透露，他们发现近日有不法分子利用 macOS 操作系统的零日漏洞，向香港一家媒体机构和一个著名民主劳工组织的网站发起攻击。攻击者利用先前披露的 XNU 漏洞（编号为 CVE-2020-27932）和相关漏洞来创建特权提升漏洞，以获取目标 Mac 机的 root 访问权限。获得 root 访问权限后，攻击者会下载一个有效负载，该负载会在受感染的 Mac 后台静默运行。谷歌安全人员指出，这是一种典型的水坑攻击，攻击者根据访问者的个人资料选择要攻陷的网站，其攻击对象是 Mac 和 iPhone 用户。安全专家表示这很可能是一起针对性的网络攻击，并且攻击团队的资源非常丰富。

② 黑客滥用 FBI 邮件服务器大规模发送虚假威胁警报

美国东海岸时间 11 月 12 日晚上，身份不明的黑客利用美国联邦调查局 (FBI) 的一台邮件服务器大规模发送垃圾邮件，发出虚假警报，谎称一场网络攻击正在发生。邮件的信息标头显示，这些邮件的发送地址为 FBI 的互联网地址。并且邮件中的“from:”部分中的域名是 eims@ic.fbi.gov，和 FBI 刑事司法信息服务 (CJIS) 相对应。FBI 的一名发言人证实称 fbi.gov 域名和互联网地址被滥用与大规模发送数万份虚假邮件警报。FBI 表示已发现这起安全事件，目前正在调查并且已关闭受陷服务器阻止垃圾邮件发送。

Copyright ©2021 奇安信CERT. All Rights Reserved.