安全热点周报

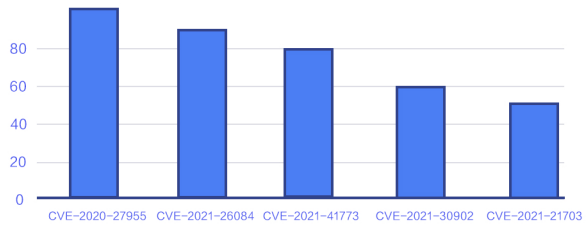
2021年11月1日　第二百一十八期

本周安全大事件

GitLab CE/EE 远程代码执行漏洞安全风险通告

近日，奇安信 CERT 监测到 GitLab CE/EE 远程代码执行漏洞（CVE-2021-22205）技术细节、PoC、EXP 均已公开，并发现在野利用。由于 GitLab 中的 ExifTool 没有正确验证用户上传的图像内容，攻击者可通过上传恶意图像文件，在图像元数据中插入恶意代码的方式利用该漏洞，成功利用此漏洞的攻击者可远程执行任意代码。经验证，GitLab CE/EE 远程代码执行漏洞（CVE-2021-22205）无需身份验证即可远程执行任意代码。由于已发现在野利用，漏洞利用的现实威胁上升。鉴于该漏洞危害较大，目前官方已有修复版本，奇安信 CERT 强烈建议客户及时自检服务器并尽快更新 GitLab 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，成功利用此漏洞的攻击者可在目标机上执行任意代码。

本周重要漏洞

注：以下漏洞为奇安信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。

漏洞编号	影响产品	危险等级	漏洞类型
CVE-2021-40865	Apache Storm	高危	远程代码执行
CVE-2021-41163	Discourse	高危	代码执行
CVE-2021-25219	BIND	高危	拒绝服务

安全事件

1　伊朗全国加油站大面积关闭，疑似网络攻击导致

10 月 26 日早上，伊朗国有天然气分销企业 NIOPDC 疑似遭到网络攻击，攻击事件导致该企业在全国范围内管理的 3500 多家加油站出现软件故障，无法正确计费收款，加油泵屏幕与油价广告牌上还显示出大量涉政异常内容。起初工作人员表示加油泵屏幕显示异常并不影响正常加油，但 NIOPDC 公司很快意识到，遭到攻击的油泵无法正确计费和收款，于是指派员工临时关停了加油站运营。伊朗石油部发言人在当天下午发布的官方声明中表示，受到影响的加油站后续会恢复运营，并未透露网络攻击的相关细节。

2　服务器故障导致韩国出现大面积断网

当地时间 10 月 25 日上午 11 点 20 分，韩国 KT 通信公司无线及有线网络服务突然中断，导致全国证券交易系统，饭店、超市结算系统，居民家中网络以及手机信号等无法正常使用，网络中断时间近 40 分钟。韩国 KT 通信公司发布声明称，当天上午出现的网络服务中断事故原因经查明为设置错误导致的服务器故障，并非此前外界猜测的遭受到了大面积分布式拒绝服务攻击（DDos）所致。并表示，故障排除后，中断的网络服务已经恢复。