国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 07 月 04 日-2022 年 07 月 10 日 **2022 年第 27 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 385 个，其中高危漏洞 107 个、中危漏洞 236 个、低危漏洞 42 个。漏洞平均分值为 5.90。本周收录的漏洞中，涉及 0day 漏洞 279 个（占 72%），其中互联网上出现“Fast Food Ordering System SQL 注入漏洞、Product Show Room Site SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 7858 个，与上周（6721 个）环比增加 17%。

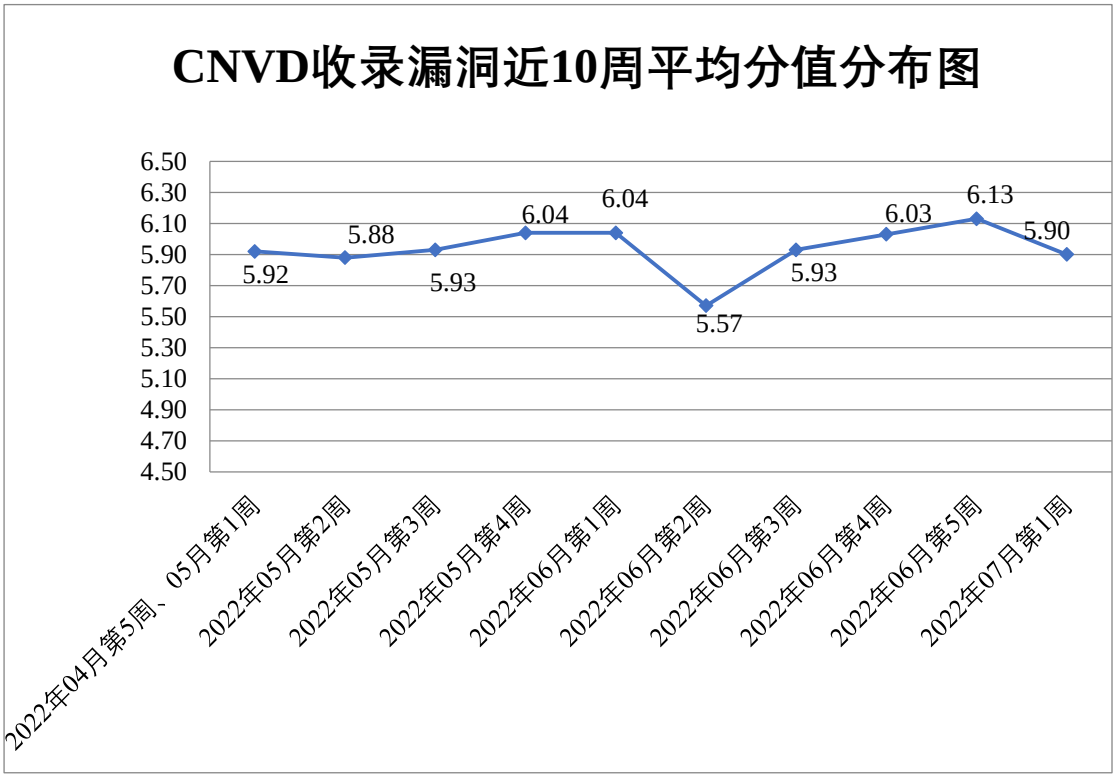

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 21 起，向基础电信企业通报漏洞事件 19 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 610 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 174 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 101 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

重庆远秋科技有限公司、智慧芽信息科技（苏州）有限公司、郑州维维信息技术有限公司、浙江淘宝网络有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、夏普商贸（中国）有限公司、暇光软件科技（上海）有限公司、温州互引信息技术有限公司、卫宁健康科技集团股份有限公司、微软（中国）有限公司、台州聚潮科技有限公司、四川易泊时捷智能科技有限公司、四川迅睿云软件开发有限公司、数字广西集团有限公司、深圳市联软科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市点晴信息技术有限公司、深圳市朝恒辉网络科技有限公司、深圳市必联电子有限公司、深圳市百为通达科技有限公司、上海瑞美信息技术有限公司、上海肯特仪表股份有限公司、上海凯京信达科技集团有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海百胜软件股份有限公司、熵基科技股份有限公司、厦门网中网软件有限公司、润申信息科技（上海）有限公司、南京九则软件科技有限公司、迈普通信技术股份有限公司、洛阳云业信息科技有限公司、罗技（中国）科技有限公司、龙归池集团有限公司、联奕科技股份有限公司、联想图像（北京）科技有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、恒锋信息科技股份有限公司、合肥市住房租赁发展股份有限公司、杭州盈高科技有限公司、杭州九麒科技有限公司、杭州海康威视数字技术股份有限公司、杭州晨科软件技术有限公司、哈尔滨伟成科技有限公司、广州易达建信科技开发有限公司、广西金中软件集团有限公司、成都智政数据科技有限公司、成都星锐蓝海网络科技有限公司、成都砺寒软件有限公司、成都驰创数码科技有限公司、北京紫荆视通科技有限公司、北京中科网威信息技术有限公司、北京中科互动科技有限公司、北京中创视讯科技有限公司、北京致远互联软件股份有限公司、北京亿华瑞成软件有限公司、北京学大信息技术集团有限公司、北京星网锐捷网络技术有限公司、北京统御至诚科技有限公司、北京搜狗信息服务有限公司、北京铭万智达科技有限公司、北京百卓网络技术有限公司、北京爱奇艺科技有限公司、暴风集团股份有限公司、安徽省科大奥锐科技有限公司、北京鼎普科技股份有限公司、中科宇图科技股份有限公司、华夏 ERP、zzcms、ZengCMS、UCMS、ThinkCMF、The Apache Software Foundation、SQLite、seacms、Rockwell Automation、QEMU、PHPEMS、

Oracle、NETGEAR、Nagios Enterprises, LLC、emlog、Emitter Studios B.V、Dolibarr、ClassCMS、Ceph、Catfish CMS、Bytebase、Adobe 和 Python Software Foundation。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司、深信服科技股份有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。贵州泰若数字科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、北京众安天下科技有限公司、杭州迪普科技股份有限公司、河南信安世纪科技有限公司、北京中百信信息技术股份有限公司、浙江大华技术股份有限公司、北京冠程科技有限公司、重庆都会信息科技有限公司、长春嘉诚信息技术股份有限公司、巨鹏信息科技有限公司、北京天地和兴科技有限公司、上海纽盾科技股份有限公司、北京安帝科技有限公司、亚信科技（成都）有限公司、杭州默安科技有限公司、北京墨云科技有限公司、杭州美创科技有限公司、山石网科通信技术股份有限公司、广州百蕴启辰科技有限公司、浙江木链物联网科技有限公司、北京升鑫网络科技有限公司及其他个人白帽子向 CNVD 提交了 7858 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、三六零数字安全科技集团有限公司、奇安信网神（补天平台）和上海交大向 CNVD 共享的白帽子报送的 5998 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数
斗象科技（漏洞盒子）	3317	3317
三六零数字安全科技集团有限公司	1851	1851
奇安信网神（补天平台）	506	506
上海交大	324	324
新华三技术有限公司	319	0
北京神州绿盟科技有限公司	311	0
北京数字观星科技有限公司	277	0
深信服科技股份有限公司	267	0
安天科技集团股份有	226	0

限公司		
北京天融信网络安全技术有限公司	167	9
天津市国瑞数码安全系统股份有限公司	115	0
厦门服云信息科技有限公司	101	0
北京启明星辰信息安全技术有限公司	80	23
恒安嘉新（北京）科技股份公司	71	1
京东科技信息技术有限公司	54	36
杭州安恒信息技术股份有限公司	41	41
内蒙古云科数据服务股份有限公司	34	34
中国电信集团系统集成有限责任公司	27	0
北京知道创宇信息技术股份有限公司	14	0
西安四叶草信息技术有限公司	9	9
深圳市腾讯计算机系统有限公司（玄武实验室）	2	2
卫士通信息产业股份有限公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	1	1
南京联成科技发展股份有限公司	1	1
北京华顺信安科技有限公司	423	0

贵州泰若数字科技有限公司	315	315
奇安星城网络安全运营服务（长沙）有限公司	62	62
河南东方云盾信息技术有限公司	17	17
北京众安天下科技有限公司	16	16
杭州迪普科技股份有限公司	14	0
河南信安世纪科技有限公司	8	8
北京中百信信息技术股份有限公司	5	5
浙江大华技术股份有限公司	4	4
北京冠程科技有限公司	4	4
重庆都会信息科技有限公司	3	3
长春嘉诚信息技术股份有限公司	3	3
巨鹏信息科技有限公司	3	3
北京天地和兴科技有限公司	3	3
上海纽盾科技股份有限公司	2	2
北京安帝科技有限公司	2	2
亚信科技（成都）有限公司	1	0
杭州默安科技有限公司	1	1

北京墨云科技有限公司	1	1
杭州美创科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
广州百蕴启辰科技有限公司	1	1
浙江木链物联网科技有限公司	1	1
北京升鑫网络科技有限公司	1	1
CNCERT 四川分中心	2	2
CNCERT 浙江分中心	2	2
个人	1244	1244
报送总计	10256	7858

本周漏洞按类型和厂商统计

本周，CNVD 收录了 385 个漏洞。WEB 应用 154 个，应用程序 113 个，网络设备（交换机、路由器等网络端设备）74 个，操作系统 27 个，智能设备（物联网终端设备）10 个，安全产品 7 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
WEB 应用	154
应用程序	113
网络设备（交换机、路由器等网络端设备）	74
操作系统	27
智能设备（物联网终端设备）	10
安全产品	7

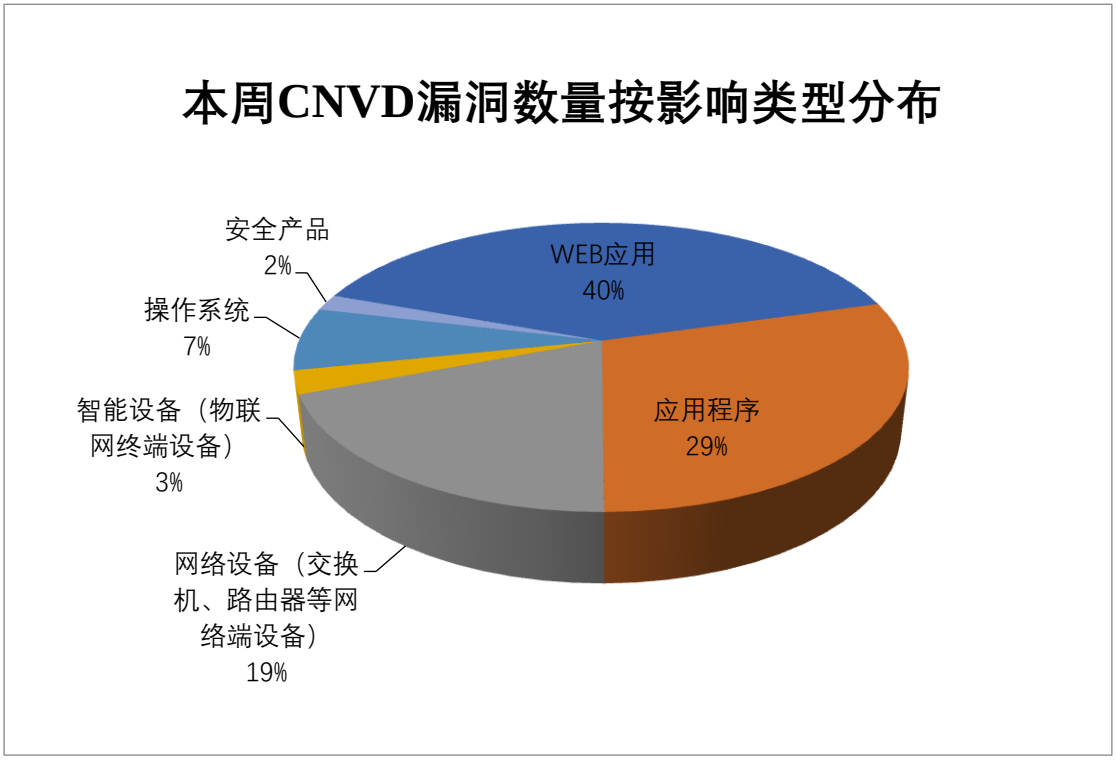

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Jenkins、D-Link、Adobe 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Jenkins	41	11%
2	D-Link	34	9%
3	Adobe	33	9%
4	Carlo Montero	17	4%
5	IBM	12	3%
6	Google	11	3%
7	Cisco	9	2%
8	WordPress	8	2%
9	中科方德软件有限公司	7	2%
10	其他	213	55%

本周行业漏洞收录情况

本周，CNVD 收录了 54 个电信行业漏洞，15 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2022-50272、CNVD-2022-50274）”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

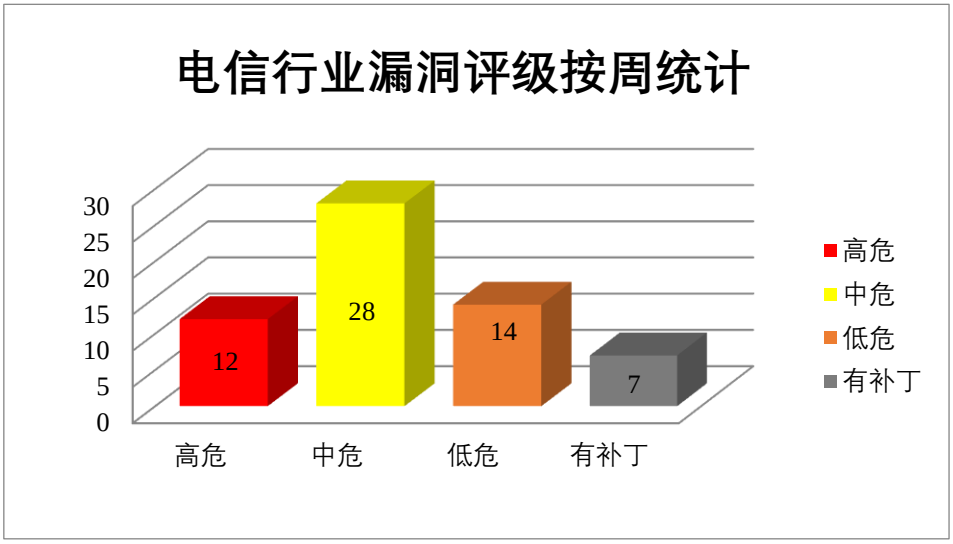

图 3 电信行业漏洞统计

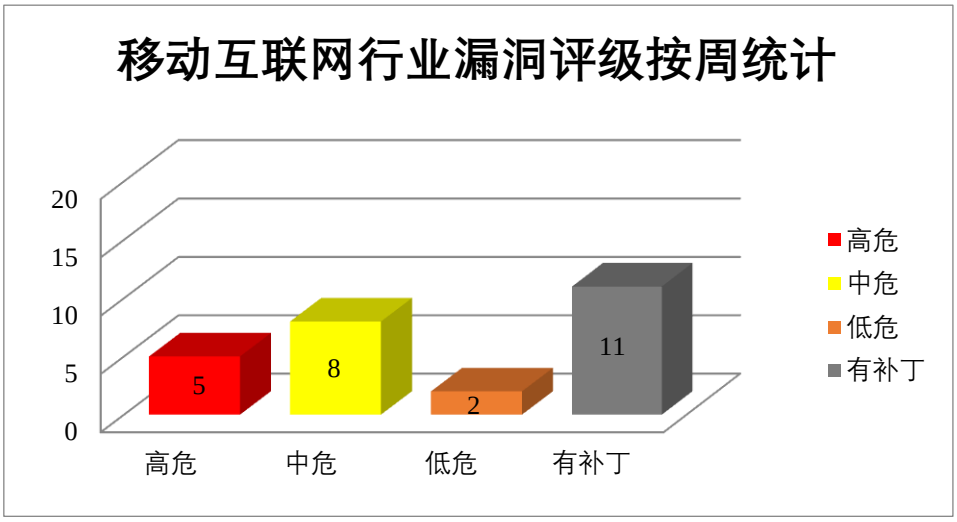

图 4 移动互联网行业漏洞统计

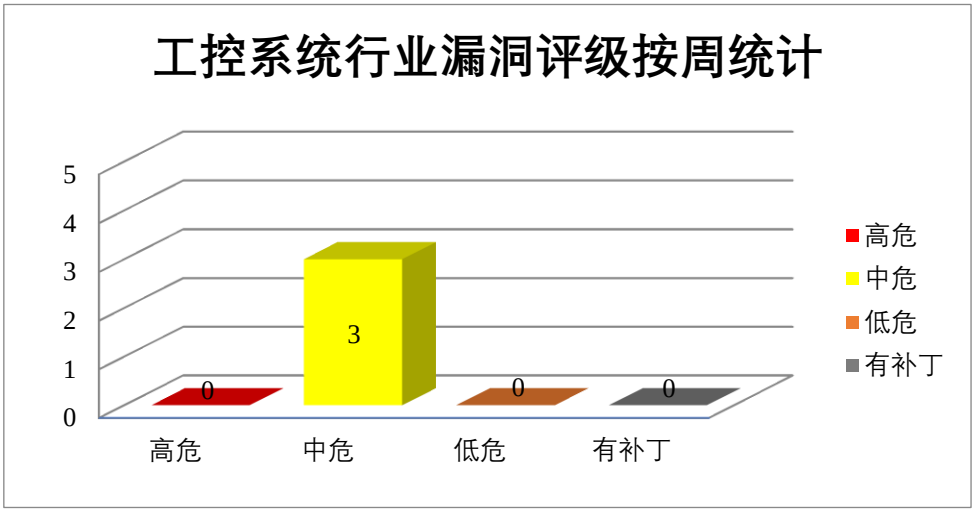

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、 Adobe 产品安全漏洞

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe InCopy 是美国 Adobe 公司的一款用于创作的文本编辑软件。Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Bridge 越界写入漏洞（CNVD-2022-50224）、Adobe InDesign 堆缓冲区溢出漏洞（CNVD-2022-50228）、Adobe InCopy 越界写入漏洞（CNVD-2022-50232、CNVD-2022-50231、CNVD-2022-50230）、Adobe Animate 越界写入漏洞（CNVD-2022-50234）、Adobe Photoshop 越界写入漏洞（CNVD-2022-50238、CNVD-2022-50239）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-50224

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50228

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50232

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50231

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50230

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50234

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50238

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50239

2、IBM 产品安全漏洞

IBM Cognos Controller 是美国 IBM 公司的一套商业智能与计划解决方案。该产品具有流程自动化、财务审计控制、创建和管理财务报告等功能。IBM Security Verify Access（ISAM）是美国 IBM 公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM App Connect Enterprise 是美国 IBM 公司的一个操作系统。IBM App Connect Enterprise 将现有业界信任的 IBM Integration Bus 技术与 IBM App Connect Professional 以及新的云本机技术进行了组合，提供一个可满足现代数字企业全面集成需求的平台。IBM Sterling Partner Engagement Manager 是美国 IBM 公司的一个自动化管理工具。IBM AIX 是美国 IBM 公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息或可能更改某些信息，导致拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM Cognos Controller 授权问题漏洞（CNVD-2022-48940、CNVD-2022-48941）、IBM Security Verify Access 输入验证错误漏洞、IBM App Connect Enterprise Certified Container 拒绝服务漏洞、IBM Sterling Partner Engagement Manager 信息泄露漏洞、IBM AIX 拒绝服务漏洞（CNVD-2022-48944、CNVD-2022-48943、CNVD-2022-48942）。其中，“IBM Cognos Controller 授权问题漏洞（CNVD-2022-48940、CNVD-2022-48941）、IBM AIX 拒绝服务漏洞（CNVD-2022-48944）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-48940

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48939

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48938

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48937

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48944

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48943

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48942

https://www.cnvd.org.cn/flaw/show/CNVD-2022-48941

3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome WebRTC 远程代码执行漏洞、Google Android 权限提升漏洞（CNVD-2022-50272、CNVD-2022-50271、CNVD-2022-50276、CNVD-2022-50274、CNVD-2022-50273）、Google Android 信息泄露漏洞（CNVD-2022-50275、CNVD-2022-50278）。其中，“Google Chrome WebRTC 远程代码执行漏洞、Google Android 权限提升漏洞（CNVD-2022-50272、CNVD-2022-50274）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-49948

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50272

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50271

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50276

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50275

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50274

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50273

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50278

4、 Cisco 产品安全漏洞

Cisco Unified Communications Manager（CUCM，Unified CM，CallManager）是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。Unified Communications Manager Session Management Edition 是 Unified Communications Manager 的会话管理版。Cisco Unity Connection 是一套语音留言平台。该平台可利用语音命令，以免提方式拨打电话或收听留言。Cisco AppDynamics Controller 是美国思科（Cisco）公司的通过跨高度分布式应用程序环境的精确跟踪和分析来监控和分析全栈数据。Cisco Smart Software Manager On-Prem 是一款用于 Cisco 产品许可证管理的组件。Cisco Smart Software Manager 是一个为用于提供许可证智能管理功能的软件。该软件消除了繁琐的产品激活密钥（PAK）和许可证文件管理，使许可证节点不再锁定到设备，可以支持任何兼容的设备上使用许可证。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取主机上的任意文件，获取敏感信息，并在易受攻击的用户浏览器中执行任意 HTML 和脚本代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Manager 任意文件读取漏洞（CNVD-2022-50625、CNVD-2022-50631）、Cisco Unified Communications Manager 跨站脚本漏洞（CNVD-2022-50628、CNVD-2022-50630）、Cisco Unified Communications Manager 和 Cisco Unity Connection 信息泄露漏洞、Cisco Unified Communications Manager 访问控制错误漏洞、Cisco AppDynamics Controller 授权问题漏洞、Cisco Smart Software Manager On-Prem 和 Cisco Smart Software Manager 资源管理错误漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，

避免引发漏洞相关的网络安全事件。

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-50625
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50628
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50627
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50626
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50632
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50631
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50630
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50629

5、Jenkins Agent Server Parameter Plugin 跨站脚本漏洞（CNVD-2022-49787）

Jenkins 和 Jenkins Plugin 都是 Jenkins 开源的产品。Jenkins 是一个应用软件。一个开源自动化服务器 Jenkins 提供了数百个插件来支持构建，部署和自动化任何项目。Jenkins Plugin 是一个应用软件。本周，Jenkins Agent Server Parameter Plugin 被披露存在跨站脚本漏洞。该漏洞源于未在显示参数的视图上对 Agent Server 参数的名称和描述进行转义，攻击者可利用该漏洞在客户端执行 JavaScript 代码。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-49787

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2022-49884	OpenSSL RSA 组件远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=4d8a88c134df634ba610ff8db1eb8478ac5fd345
CNVD-2022-50229	Adobe InDesign 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/indesign/apsb21-73.html
CNVD-2022-49948	Google Chrome WebRTC 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2022/07/extended-stable-channel-update-for.html
CNVD-2022-49949	Atlassian Jira Server and Data Center 服务器端请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://confluence.atlassian.com/jira/j

			ira-server-security-advisory-29th-june-2022-1142430667.html
CNVD-2022-49973	Apache Commons 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/tdf5n7j80lfxdhs2764vn0xmpfodm87s
CNVD-2022-50231	Adobe InCopy 越界写入漏洞（CNVD-2022-50231）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/incopy/apsb22-29.html
CNVD-2022-50272	Google Android 权限提升漏洞（CNVD-2022-50272）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/pixel/2022-06-01?hl=en
CNVD-2022-48944	IBM AIX 拒绝服务漏洞（CNVD-2022-48944）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com
CNVD-2022-50233	Adobe InCopy 堆缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/incopy/apsb22-29.html
CNVD-2022-50280	Google Android 权限提升漏洞（CNVD-2022-50280）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2022-06-01

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。此外，IBM、Google、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，读取主机上的任意文件，获取敏感信息，执行任意代码，导致拒绝服务攻击等。另外，Jenkins Agent Server Parameter Plugin 被披露存在跨站脚本漏洞。攻击者可利用该漏洞在客户端执行 JavaScript 代码。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、Fast Food Ordering System SQL 注入漏洞

验证描述

Fast Food Ordering System 是 Carlo Montero 个人开发者的一个快餐订购系统。

Fast Food Ordering System 1.0 版本存在 SQL 注入漏洞，该漏洞源于/ffos/admin/menus/view_menu.php?id=页面缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执

行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/k0xx11/bug_report/blob/main/vendors/oretnom23/fast-food-ordering-system/SQLi-6.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-48951

信息提供者

新华三技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. Django 网络框架的一个 SQL 注入漏洞已被修复

Django 项目背后的开发团队已经解决了其框架中存在的一个 SQL 注入漏洞，该开发团队还发布了安全补丁，作为升级到最新版本之前的临时解决方案。

参考链接：https://securityaffairs.co/wordpress/132853/security/django-framework-sql-injection.html

2. Chrome 被爆零日漏洞，谷歌督促用户尽快更新

近期，谷歌发布公告，称已经为 Windows 用户发布了 Chrome 103.0.5060.114 更新，以解决在野被攻击者利用的零日漏洞，这也是 2022 年谷歌修补的第四个 Chrome 零日漏洞。目前 103.0.5060.114 版本正在全球范围内的 Stable Desktop 频道推出，谷歌表示需要几天或几周的时间才能触达整个用户群。

参考链接：https://www.freebuf.com/news/338299.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等

工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537