# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2023 年 10 月 30 日-2023 年 11 月 05 日** **2023 年第 44 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 425 个，其中高危漏洞 177 个、中危漏洞 229 个、低危漏洞 19 个。漏洞平均分值为 6.34。本周收录的漏洞中，涉及 0day 漏洞 364 个（占 86%），其中互联网上出现“Geeklog grp_desc 参数跨站脚本漏洞、PortlandLabs Concrete CMS 跨站脚本漏洞”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漏洞总数 20305 个，与上周（12213 个）环比增多 66%。

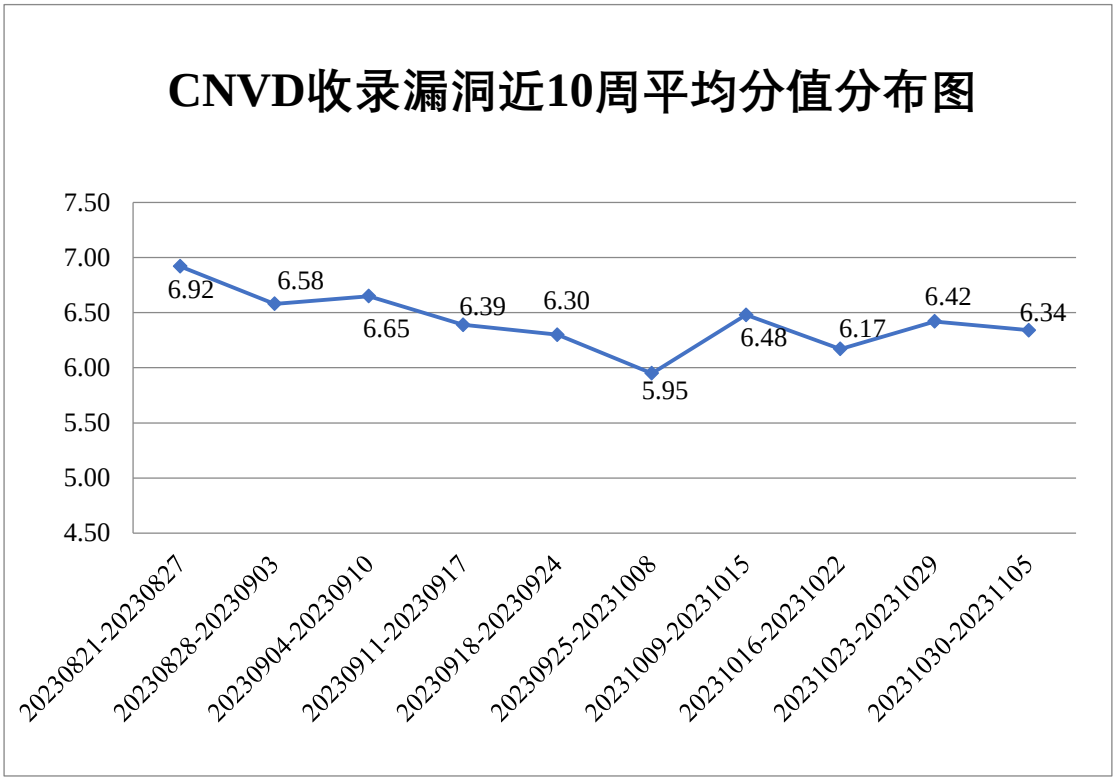


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 34 起，向基础电信企业通报漏洞事件 17 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 1084 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 122 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 45 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：

珠海市蜂巢数据技术有限公司、珠海派诺科技股份有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、重庆泛普软件有限公司、浙江知水信息技术有限公司、浙江云马智慧科技有限公司、浙江托普云农科技股份有限公司、浙江花田网络有限公司、浙江和仁科技股份有限公司、长沙友点软件科技有限公司、长沙格子教育咨询有限公司、长沙德尚网络科技有限公司、云南云天化信息科技有限公司、粤港澳大湾区数字经济研究院（福田）、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、扬子江药业集团有限公司、信阳奇鸟网络科技有限公司、信呼、校无忧科技网络公司、夏普商贸（中国）有限公司、西安众邦网络科技有限公司、西安匀速攻网络科技有限公司、武汉天地伟业科技有限公司、武汉达梦数据库有限公司、无锡安腾软件开发有限公司、潍坊家园驿站电子技术有限公司、天津津云新媒体集团股份有限公司、天津黑核科技有限公司、台铃科技（深圳）有限公司、苏州科达科技股份有限公司、苏州浩辰软件股份有限公司、四平市九州易通科技有限公司、四川希望教育产业集团有限公司、世邦通信股份有限公司、昇频股份有限公司、神州数码控股有限公司、深圳市优卡特实业有限公司、深圳市唯传科技有限公司、深圳市思迅软件股份有限公司、深圳市蓝凌软件股份有限公司、深圳市捷道智控实业有限公司、深圳市家家顺物联科技有限公司、深圳市吉祥腾达科技有限公司、深圳市飞速创新技术股份有限公司、深圳市博思协创网络科技有限公司、深圳柒芮斯珠宝网络科技有限公司、申瓯通信设备有限公司、上海盛代信息科技有限公司、上海穆云智能科技有限公司、上海寰创通信科技股份有限公司、上海翰临电子科技有限公司、上海泛微网络科技股份有限公司、上海豹云网络信息服务有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、商派软件有限公司、山西企凝信息科技有限公司、山西点可云科技有限公司、厦门圆古网络科技有限公司、厦门四信通信科技有限公司、厦门能加新能源科技有限公司、三星（中国）投资有限公司、普联技术有限公司、南京小牛智能科技有限公司、明腾网络股份有限公司、蓝盾信息安全技术有限公司、津鸿软通联信息技术有限公司、金蝶软件（中国）有限公司、江苏四目网络科技有限公司、江苏三恒科技股份有限公司、江苏麦维智能科技有限公司、建信住房服务有限责任公司、吉翁电子（深圳）有限公司、吉首市微商互联信息技术有限公司、惠普贸易（上海）有限公司、淮南市银泰软件科技有限公司、华农智联（北京）信

息科技有限公司、华创信诚（北京）网络信息技术有限公司、湖南翱云网络科技有限公司、合肥彼岸互联信息技术有限公司、杭州易软共创网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州新视窗信息技术有限公司、杭州顺网科技股份有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、杭州堆栈科技有限公司、杭州迪普科技股份有限公司、杭州德联科技股份有限公司、哈尔滨伟成科技有限公司、国可工软科技有限公司、广州信虹通信技术有限公司、广州网易计算机系统有限公司、广州图创计算机软件开发有限公司、广州华的网络科技有限公司、广州红帆科技有限公司、广联达科技股份有限公司、广东数夫软件有限公司、广东深蓝智能软件有限公司、广东广凌信息科技股份有限公司、广东保伦电子股份有限公司、福建亿能达信息技术股份有限公司、泛微网络科技股份有限公司、东莞市通天星软件科技有限公司、东莞市凝聚力软件开发服务有限公司、东北师大理想软件股份有限公司、鼎点视讯科技有限公司、顶点软件股份有限公司、丹东鸭绿江网络技术有限公司、大唐电信科技股份有限公司、大连金马衡器有限公司、成都友加畅捷科技有限公司、成都虚谷伟业科技有限公司、成都星锐蓝海网络科技有限公司、成都集致生活科技有限公司、成都积微物联电子商务有限公司、畅捷通信息技术股份有限公司、禅道软件（青岛）有限公司、碧桂园生活服务集团股份有限公司、北京子在川上科技有限公司、北京卓正志远软件有限公司、北京卓软在线信息技术有限公司、北京中庆现代技术股份有限公司、北京中科聚网信息技术有限公司、北京致远互联软件股份有限公司、北京云帆互联科技有限公司、北京用友政务软件股份有限公司、北京亿赛通科技发展有限责任公司、北京怡生乐居信息服务有限公司、北京星网锐捷网络技术有限公司、北京新起点盛和教育科技有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京天润顺腾科技有限公司、北京牛电科技有限责任公司、北京朗新天霁软件技术有限公司、北京火山引擎科技有限公司、北京鸿湾科技发展有限公司、北京宏景世纪软件股份有限公司、北京和欣运达科技有限公司、北京冠群信息技术股份有限公司、北京博图纵横科技有限责任公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、百家 CMS 微商城、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、爱普生（中国）有限公司、SEMCMS 和 seacms。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、北京启明星辰信息安全技术有限公司、新华三技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。联想集团、安徽锋刃信息科技有限公司、快页信息技术有限公司、中孚安全技术有限公司、河南东方云盾信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、北京中关村实验室、湖南泛联新安信息科技有限公司、内

蒙古洞明科技有限公司、赛尔网络有限公司、江苏金盾检测技术股份有限公司、智网安云（武汉）信息技术有限公司、河南灵创电子科技有限公司、江苏晟晖信息科技有限公司、北京山石网科信息技术有限公司、西藏熙安信息技术有限责任公司、贵州多彩网安科技有限公司、北京微步在线科技有限公司、超聚变数字技术有限公司、平安银河实验室、山石网科通信技术股份有限公司、浙江中控技术股份有限公司、北京永洪商智科技有限公司、比亚迪股份有限公司、南京深安科技有限公司、北京君云天下科技有限公司、上海直画科技有限公司、郑州埃文计算机科技有限公司、江苏极元信息技术有限公司、黑龙江亿林网络股份有限公司、合肥梆梆信息科技有限公司、卫士通（广州）信息安全技术有限公司、山东云天安全技术有限公司、工业和信息化部电子第五研究所、河南悦海数安科技有限公司、杭州海康威视数字技术股份有限公司、杭州默安科技有限公司、亚信科技（成都）有限公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 20305 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 17866 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 |
|---|---|---|
| 奇安信网神（补天平台） | 13532 | 13532 |
| 斗象科技（漏洞盒子） | 3350 | 3350 |
| 北京天融信网络安全技术有限公司 | 1539 | 19 |
| 北京启明星辰信息安全技术有限公司 | 752 | 2 |
| 新华三技术有限公司 | 662 | 0 |
| 北京神州绿盟科技有限公司 | 641 | 307 |
| 三六零数字安全科技集团有限公司 | 549 | 549 |
| 上海交大 | 435 | 435 |
| 北京数字观星科技有限公司 | 369 | 0 |
| 安天科技集团股份有限公司 | 238 | 0 |
| 天津市国瑞数码安全系统股份有限公司 | 219 | 0 |

| | | |
|---|---|---|
| 深信服科技股份有限公司 | 179 | 6 |
| 阿里云计算有限公司 | 139 | 7 |
| 杭州安恒信息技术股份有限公司 | 123 | 44 |
| 京东科技信息技术有限公司 | 45 | 45 |
| 杭州迪普科技股份有限公司 | 25 | 0 |
| 南京联成科技发展股份有限公司 | 20 | 20 |
| 中国电信集团系统集成有限责任公司 | 12 | 1 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 8 | 8 |
| 北京长亭科技有限公司 | 6 | 6 |
| 西安四叶草信息技术有限公司 | 5 | 5 |
| 贵州泰若数字科技有限公司 | 3 | 3 |
| 中国电信股份有限公司网络安全产品运营中心 | 3 | 3 |
| 浙江大华技术股份有限公司 | 2 | 2 |
| 北京智游网安科技有限公司 | 2 | 2 |
| 中电科网络安全科技股份有限公司 | 1 | 1 |
| 北京安信天行科技有限公司 | 1 | 1 |
| 华为技术有限公司 | 1 | 1 |
| 北京知道创宇信息技 | 1 | 0 |

| | | |
|---|---|---|
| 术股份有限公司 | | |
| 联想集团 | 58 | 58 |
| 安徽锋刃信息科技有限公司 | 51 | 51 |
| 亚信科技（成都）有限公司 | 45 | 45 |
| 快页信息技术有限公司 | 42 | 42 |
| 中孚安全技术有限公司 | 39 | 39 |
| 河南东方云盾信息技术有限公司 | 34 | 34 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 32 | 32 |
| 北京中关村实验室 | 22 | 22 |
| 湖南泛联新安信息科技有限公司 | 18 | 18 |
| 内蒙古洞明科技有限公司 | 15 | 15 |
| 赛尔网络有限公司 | 13 | 13 |
| 江苏金盾检测技术股份有限公司 | 11 | 11 |
| 智网安云（武汉）信息技术有限公司 | 9 | 9 |
| 河南灵创电子科技有限公司 | 8 | 8 |
| 江苏晟晖信息科技有限公司 | 7 | 7 |
| 北京山石网科信息技术有限公司 | 6 | 6 |
| 西藏熙安信息技术有限责任公司 | 5 | 5 |
| 贵州多彩网安科技有限公司 | 5 | 5 |

| | | |
|---|---|---|
| 北京微步在线科技有限公司 | 3 | 3 |
| 超聚变数字技术有限公司 | 3 | 3 |
| 平安银河实验室 | 3 | 3 |
| 山石网科通信技术股份有限公司 | 3 | 3 |
| 浙江中控技术股份有限公司 | 2 | 2 |
| 北京永洪商智科技有限公司 | 2 | 2 |
| 比亚迪股份有限公司 | 2 | 2 |
| 南京深安科技有限公司 | 2 | 2 |
| 北京君云天下科技有限公司 | 2 | 2 |
| 上海直画科技有限公司 | 2 | 2 |
| 郑州埃文计算机科技有限公司 | 2 | 2 |
| 江苏极元信息技术有限公司 | 1 | 1 |
| 黑龙江亿林网络股份有限公司 | 1 | 1 |
| 合肥梆梆信息科技有限公司 | 1 | 1 |
| 卫士通（广州）信息安全技术有限公司 | 1 | 1 |
| 山东云天安全技术有限公司 | 1 | 1 |
| 工业和信息化部电子第五研究所 | 1 | 1 |
| 河南悦海数安科技有限公司 | 1 | 1 |
| 杭州海康威视数字技 | 1 | 1 |

| | | |
|---|---|---|
| 术股份有限公司 | | |
| 杭州默安科技有限公司 | 1 | 1 |
| 任子行网络技术股份有限公司 | 1 | 1 |
| CNCERT 广西分中心 | 6 | 6 |
| CNCERT 宁夏分中心 | 2 | 2 |
| CNCERT 内蒙古分中心 | 2 | 2 |
| 个人 | 1490 | 1490 |
| 报送总计 | 24818 | 20305 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 425 个漏洞。WEB 应用 237 个，应用程序 97 个，网络设备（交换机、路由器等网络端设备）58 个，操作系统 21 个，智能设备（物联网终端设备）11 个，安全产品 1 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 | 237 |
| 应用程序 | 97 |
| 网络设备（交换机、路由器等网络端设备） | 58 |
| 操作系统 | 21 |
| 智能设备（物联网终端设备） | 11 |
| 安全产品 | 1 |

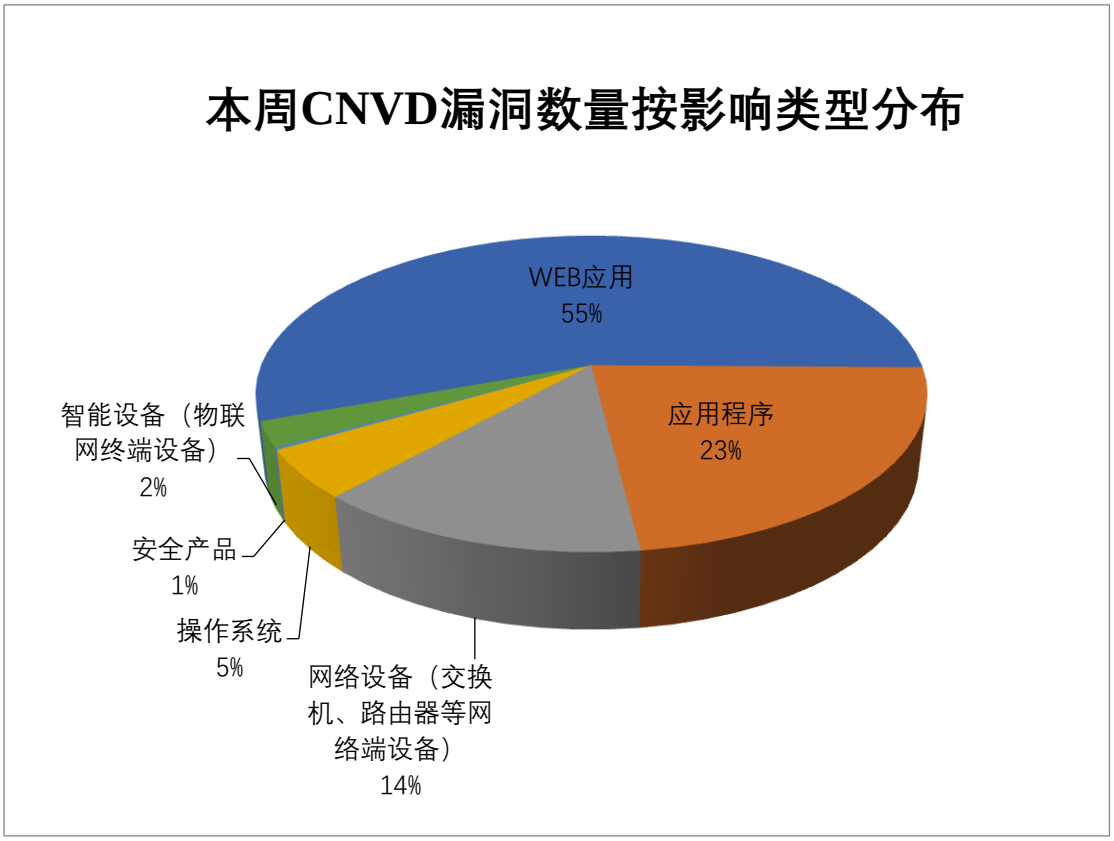


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及北京百卓网络技术有限公司、用友网络科技股份有限公司、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 | 北京百卓网络技术有限公司 | 20 | 5% |
| 2 | 用友网络科技股份有限公司 | 16 | 4% |
| 3 | Adobe | 15 | 4% |
| 4 | Google | 12 | 3% |
| 5 | F5 | 11 | 3% |
| 6 | TOTOLINK | 10 | 2% |
| 7 | Microsoft | 9 | 2% |
| 8 | D-Link | 9 | 2% |
| 9 | WordPress | 6 | 1% |
| 10 | 其他 | 317 | 74% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 37 个电信行业漏洞，49 个移动互联网行业漏洞，4 个工控行

业漏洞（如下图所示）。其中，“Google Android onCreate 模块授权问题漏洞、Google Android 权限提升漏洞（CNVD-2023-82067）”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/

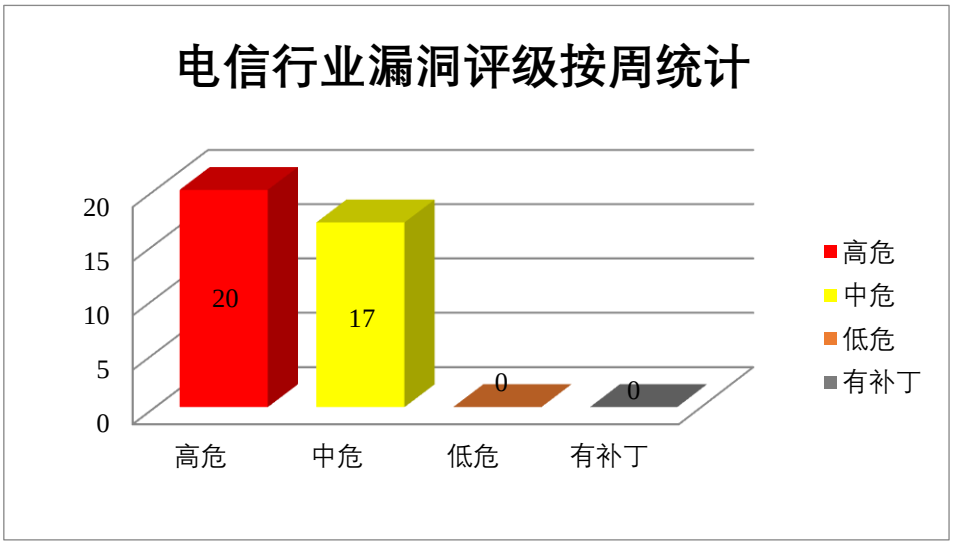


图 3 电信行业漏洞统计

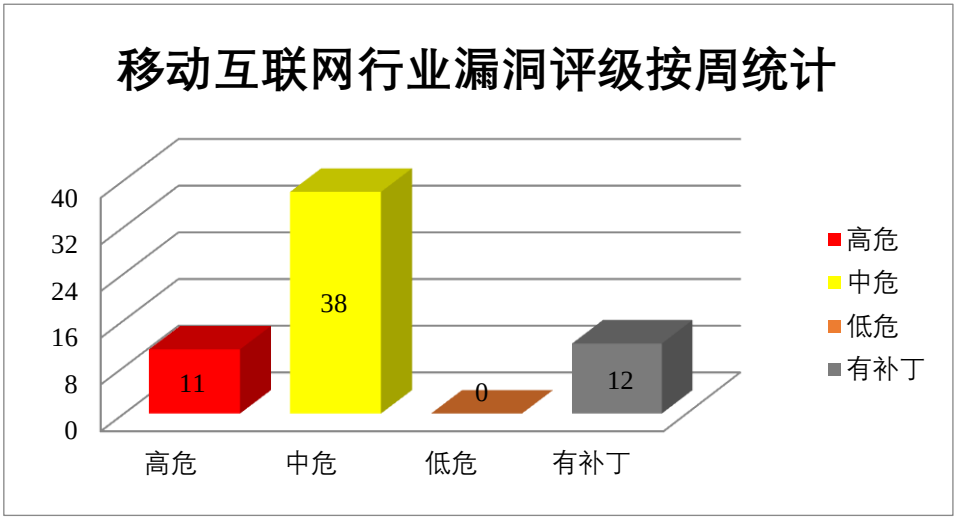


图 4 移动互联网行业漏洞统计

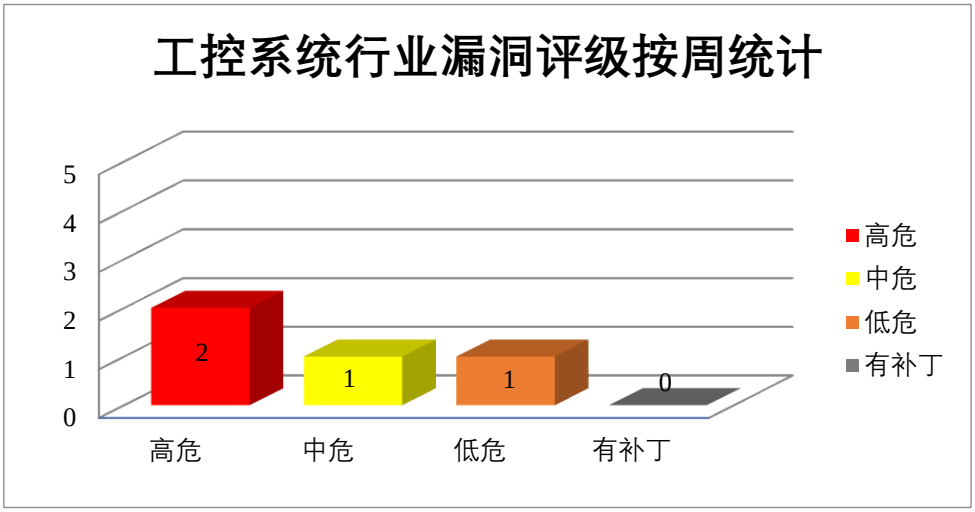


图 5 工控系统行业漏洞统计

## 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、Google 产品安全漏洞

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，攻击者可利用漏洞在系统上执行任意代码，获得提升的特权。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-82060、CNVD-2023-82061、CNVD-2023-82066、CNVD-2023-82067、CNVD-2023-82070）、Google Android 代码执行漏洞（CNVD-2023-82068、CNVD-2023-82071）、Google Android onCreate 模块授权问题漏洞。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-2023-82060

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82061

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82062

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82066

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82067

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82068

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82070

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82071

### 2、F5 产品安全漏洞

F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载

均衡等功能的应用交付平台。F5 BIG-IQ Centralized Management 是美国 F5 公司的一套基于软件的云管理解决方案。该方案支持跨公共和私有云、传统数据中心和混合环境部署应用交付和网络服务。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，修改 BIG-IP 边缘客户端的请求和响应，在系统上执行任意系统命令，导致进程终止等。

CNVD 收录的相关漏洞包括：F5 BIG-IP 远程代码执行漏洞（CNVD-2023-82300）、F5 BIG-IP 和 BIG-IQ Centralized Management 拒绝服务漏洞、F5 BIG-IP 信息泄露漏洞（CNVD-2023-82304）、F5 BIG-IP Edge Client for Windows 和 macOS 安全绕过漏洞（CNVD-2023-82305、CNVD-2023-82306）、F5 BIG-IP 拒绝服务漏洞（CNVD-2023-82307）、F5 BIG-IP 路径遍历漏洞（CNVD-2023-82309）、F5 BIG-IP 资源管理错误漏洞。其中，“F5 BIG-IP 远程代码执行漏洞（CNVD-2023-82300）、F5 BIG-IP Edge Client for Windows 和 macOS 安全绕过漏洞（CNVD-2023-82306）、F5 BIG-IP 拒绝服务漏洞（CNVD-2023-82307）”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-2023-82300
https://www.cnvd.org.cn/flaw/show/CNVD-2023-82303
https://www.cnvd.org.cn/flaw/show/CNVD-2023-82304
https://www.cnvd.org.cn/flaw/show/CNVD-2023-82305
https://www.cnvd.org.cn/flaw/show/CNVD-2023-82306
https://www.cnvd.org.cn/flaw/show/CNVD-2023-82307
https://www.cnvd.org.cn/flaw/show/CNVD-2023-82309
https://www.cnvd.org.cn/flaw/show/CNVD-2023-82310

### 3、Adobe 产品安全漏洞

Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe Media Encoder 是美国奥多比（Adobe）公司的一款音、视频编码应用程序。Adobe Connect 是美国奥多比（Adobe）公司的一个用于创建会议环境的软件。Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问未经授权的数据，在系统上执行任意代码或者导致拒绝服务等。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2023-82284）、Adobe InDesign 缓冲区溢出漏洞（CNVD-2023-82288）、Adobe Media

Encoder 缓冲区溢出漏洞（CNVD-2023-82287）、Adobe Connect 跨站脚本漏洞（CNVD-2023-82286）、Adobe Acrobat and Reader 越界读取漏洞（CNVD-2023-82289）、Adobe Commerce 授权问题漏洞（CNVD-2023-82676）、Adobe Commerce 跨站脚本漏洞（CNVD-2023-82675）、Adobe Commerce SQL 注入漏洞。其中，“Adobe InDesign 缓冲区溢出漏洞（CNVD-2023-82288）、Adobe Commerce 授权问题漏洞（CNVD-2023-82676）、Adobe Commerce 跨站脚本漏洞（CNVD-2023-82675）”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-2023-82284

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82288

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82287

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82286

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82289

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82676

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82675

https://www.cnvd.org.cn/flaw/show/CNVD-2023-82674

### 4、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞远程执行代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Layer 2 Tunneling Protocol 远程代码执行漏洞（CNVD-2023-81880、CNVD-2023-81879、CNVD-2023-81878、CNVD-2023-81883、CNVD-2023-81882、CNVD-2023-81881、CNVD-2023-81885、CNVD-2023-81884）。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-2023-81880

https://www.cnvd.org.cn/flaw/show/CNVD-2023-81879

https://www.cnvd.org.cn/flaw/show/CNVD-2023-81878

https://www.cnvd.org.cn/flaw/show/CNVD-2023-81883

https://www.cnvd.org.cn/flaw/show/CNVD-2023-81882

https://www.cnvd.org.cn/flaw/show/CNVD-2023-81881

https://www.cnvd.org.cn/flaw/show/CNVD-2023-81885

https://www.cnvd.org.cn/flaw/show/CNVD-2023-81884

### 5、TeleAdapt RoomCast TA-2400 信任管理问题漏洞

TeleAdapt RoomCast TA-2400 是英国 TeleAdapt 公司的一款适用于客房的一体化、自带的顶级内容流媒体盒。本周，TeleAdapt RoomCast TA-2400 被披露存在信任管理问

题漏洞。攻击者可利用该漏洞伪造密钥。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-2023-83069

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

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-2023-81878 | Microsoft Windows Layer 2 Tunneling Protocol 远程代码执行漏洞（CNVD-2023-81878） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41765 |
| CNVD-2023-82062 | Google Android onCreate 模块授权问题漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2023-08-01 |
| CNVD-2023-82288 | Adobe InDesign 缓冲区溢出漏洞（CNVD-2023-82288） | 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/apsb23-38.html |
| CNVD-2023-82300 | F5 BIG-IP 远程代码执行漏洞（CNVD-2023-82300） | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：https://my.f5.com/manage/s/article/K000137353 |
| CNVD-2023-82676 | Adobe Commerce 授权问题漏洞（CNVD-2023-82676） | 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/magento/apsb23-50.html |
| CNVD-2023-81881 | Microsoft Windows Layer 2 Tunneling Protocol 远程代码执行漏洞（CNVD-2023-81881） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41773 |
| CNVD-2023-82066 | Google Android 权限提升漏洞（CNVD-2023-82066） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2023-08-01 |
| CNVD-2023-82307 | F5 BIG-IP 拒绝服务漏洞（CNVD-2023-82307） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://my.f5.com/manage/s/article/K20145107 |
| CNVD-2023-82068 | Google Android 代码执行漏洞（CNVD-2023-82068） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新： |

| | | | |
|---|---|---|---|
| | | | https://source.android.com/security/bulletin/2023-08-01 |
| CNVD-2023-81886 | Microsoft Windows Layer 2 Tunneling Protocol 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41771 |

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码，获得提升的特权。此外，F5、Adobe、Microsoft 等多款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，修改 BIG-IP 边缘客户端的请求和响应，在系统上执行任意系统命令，导致拒绝服务等。另外，TeleAdapt RoomCast TA-2400 被披露存在信任管理问题漏洞。攻击者可利用该漏洞伪造密钥。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、Geeklog grp_desc 参数跨站脚本漏洞

**验证描述**

Geeklog 是免费开源的博客软件。

Geeklog grp_desc 参数存在跨站脚本漏洞，该漏洞是由于 public_html/admin/group.php 脚本对用户提供的输入进行了不正确的验证。攻击者可利用该漏洞窃取受害者基于 cookie 的身份验证凭据。

**验证信息**

POC 链接：https://github.com/CrownZTX/vulnerabilities/blob/main/geeklog/Stored_XSS_in_group.php.md/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-83044

**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. Lazarus 集团利用已知漏洞攻击软件供应商

Lazarus 集团被认为是一场新活动的幕后黑手，在该活动中，一家未透露姓名的软

件供应商通过利用另一款备受瞩目的软件中的已知安全漏洞而受到损害。

参考链接：https://www.anquanke.com/post/id/291090

### 2. 利用 Apache ActiveMQ 漏洞的 HelloKitty 勒索软件组织

网络安全研究人员警告说，涉嫌利用 Apache ActiveMQ 开源消息代理服务中最近披露的关键安全漏洞，该漏洞可能导致远程代码执行。

参考链接：https://thehackernews.com/2023/11/hellokitty-ransomware-group-exploiting.html

### 关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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国家网络安全漏洞库，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，是我国计算机网络应急处理体系中的牵头单位。

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