国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 01 月 02 日-2023 年 01 月 08 日 **2023 年第 1 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 346 个，其中高危漏洞 112 个、中危漏洞 208 个、低危漏洞 26 个。漏洞平均分值为 6.15。本周收录的漏洞中，涉及 0day 漏洞 290 个（占 84%），其中互联网上出现“Zettlr 输入验证错误漏洞、WordPress Transposh WordPress Translation 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 4085 个，与上周（47744 个）环比减少 91%。

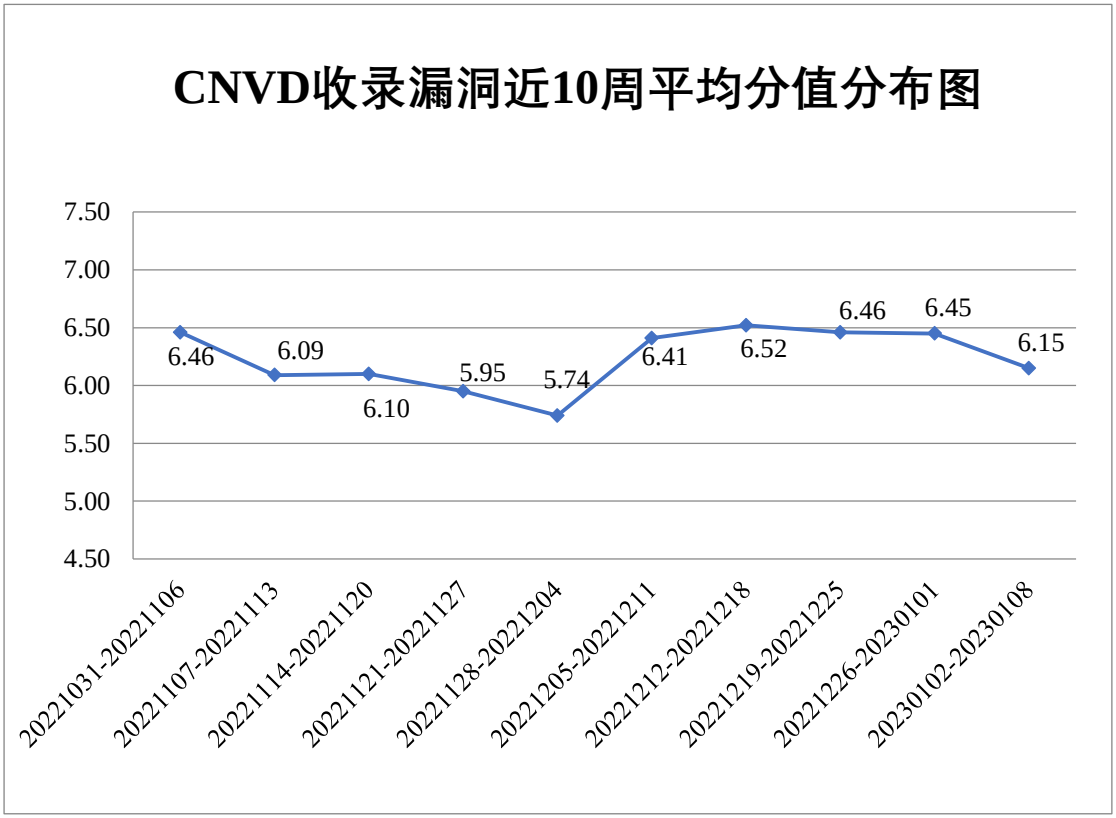

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 27 起，向基础电信企业通报漏洞事件 38 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 94 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 27 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 57 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：

郑州金鼓通信技术有限公司、浙江中控技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、义乌中国小商品城大数据有限公司、新天科技股份有限公司、夏普商贸（中国）有限公司、武汉城投停车场投资建设管理有限公司、无锡信捷电气股份有限公司、天津来去智运科技有限公司、随锐科技集团股份有限公司、深圳市牙杉科技有限公司、深圳市思迅软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市顶讯网络科技有限公司、深圳市丛文安全电子有限公司、深圳市朝恒辉网络科技有限公司、上海卓卓网络科技有限公司、上海瑞美信息技术有限公司、上海企望信息科技有限公司、商派软件有限公司、山东欧倍尔软件科技有限责任公司、厦门一指通智能科技有限公司、鹏为软件股份有限公司、浪潮电子信息产业股份有限公司、廊坊市极致网络科技有限公司、昆明创林科技有限公司、劲旅环境科技股份有限公司、佳能（中国）有限公司、杭州跃翔科技有限公司、杭州海康威视数字技术股份有限公司、海尔集团电子商务有限公司、广州图创计算机软件开发有限公司、广州宸瑞软件科技有限公司、福建星网锐捷通讯股份有限公司、东华软件股份公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京小桔科技有限公司、北京金和网络股份有限公司、北京春雨天下软件有限公司、北京百卓网络技术有限公司、安徽科迅教育装备集团有限公司、阿里巴巴集团安全应急响应中心和 AVEVA。

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、北京启明星辰信息安全技术有限公司、西安四叶草信息技术有限公司、深信服科技股份有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。赛尔网络有限公司、上海齐同信息科技有限公司、快页信息技术有限公司、山东云天安全技术有限公司、河南东方云盾信息技术有限公司、博智安全科技股份有限公司、杭州美创科技有限公司、北京网猿科技有限公司、杭州默安科技有限公司、河南灵创电子科技有限公司、听潮盛世（北京）科技有限公司、安徽锋刃信息科技有限公司、重庆都会信息科技、苏州棱镜七彩信息科技有限公司、北京山石网科信息技术有限公司、中通服创发科技有限责任公司、浙江东

安检测技术有限公司、北京微步在线科技有限公司、北京宇天恒瑞科技发展有限公司、江苏保旺达软件技术有限公司、山东九域信息技术有限公司、广州安亿信软件科技有限公司、河南悦海数安科技有限公司、重庆易阅科技有限公司、河南天祺信息安全技术有限公司、广东蓝爵网络安全技术股份有限公司、新疆海狼科技有限公司、中国人寿保险股份有限公司、浙江大学控制科学与工程学院、广西等保安全测评有限公司、北京时代新威信息技术有限公司、郑州埃文科技、山东正中信息技术股份有限公司、山东道普测评技术有限公司、河北镌远网络科技有限公司、神州灵云（北京）科技有限公司及其他个人白帽子向 CNVD 提交了 4085 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）、奇安信网神（补天平台）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 2802 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
三六零数字安全科技集团有限公司	1051	1051
奇安信网神（补天平台）	1028	1028
斗象科技（漏洞盒子）	484	484
上海交大	239	239
新华三技术有限公司	142	0
北京启明星辰信息安全技术有限公司	140	0
西安四叶草信息技术有限公司	124	124
深信服科技股份有限公司	88	0
恒安嘉新（北京）科技股份公司	72	0
北京数字观星科技有限公司	62	0
天津市国瑞数码安全系统股份有限公司	59	0
南京众智维信息科技有限公司	37	37
中国电信集团系统集成有限责任公司	31	1

京东科技信息技术有限公司	22	11
远江盛邦（北京）网络安全科技股份有限公司	19	19
杭州安恒信息技术股份有限公司	16	16
北京长亭科技有限公司	10	10
浙江大华技术股份有限公司	5	5
北京天融信网络安全技术有限公司	4	4
北京知道创宇信息技术股份有限公司	2	0
北京信联科汇科技有限公司	1	1
赛尔网络有限公司	103	103
上海齐同信息科技有限公司	61	61
快页信息技术有限公司	37	37
山东云天安全技术有限公司	23	23
河南东方云盾信息技术有限公司	19	19
博智安全科技股份有限公司	18	18
杭州美创科技有限公司	15	15
北京网猿科技有限公司	15	15
杭州默安科技有限公司	13	13
河南灵创电子科技有	10	10

限公司		
听潮盛世（北京）科技有限公司	6	6
安徽锋刃信息科技有限公司	6	6
重庆都会信息科技	5	5
苏州棱镜七彩信息科技有限公司	5	5
北京山石网科信息技术有限公司	5	5
中通服创发科技有限责任公司	4	4
浙江东安检测技术有限公司	3	3
北京微步在线科技有限公司	3	3
北京宇天恒瑞科技发展有限公司	3	3
江苏保旺达软件技术有限公司	3	3
山东九域信息技术有限公司	3	3
广州安亿信软件科技有限公司	2	2
河南悦海数安科技有限公司	2	2
重庆易阅科技有限公司	1	1
河南天祺信息安全技术有限公司	1	1
广东蓝爵网络安全技术股份有限公司	1	1
新疆海狼科技有限公司	1	1
中国人寿保险股份有	1	1

限公司		
浙江大学控制科学与工程学院	1	1
广西等保安全测评有限公司	1	1
北京时代新威信息技术有限公司	1	1
郑州埃文科技	1	1
山东正中信息技术股份有限公司	1	1
山东道普测评技术有限公司	1	1
河北镌远网络科技有限公司	1	1
神州灵云（北京）科技有限公司	1	1
CNCERT 四川分中心	5	5
个人	673	673
报送总计	4691	4085

本周漏洞按类型和厂商统计

本周，CNVD 收录了 346 个漏洞。WEB 应用 152 个，网络设备（交换机、路由器等网络端设备）75 个，应用程序 69 个，智能设备（物联网终端设备）30 个，操作系统 13 个，数据库 4 个，安全产品 3 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	152
网络设备（交换机、路由器等网络端设备）	75
应用程序	69
智能设备（物联网终端设备）	30
操作系统	13
数据库	4
安全产品	3

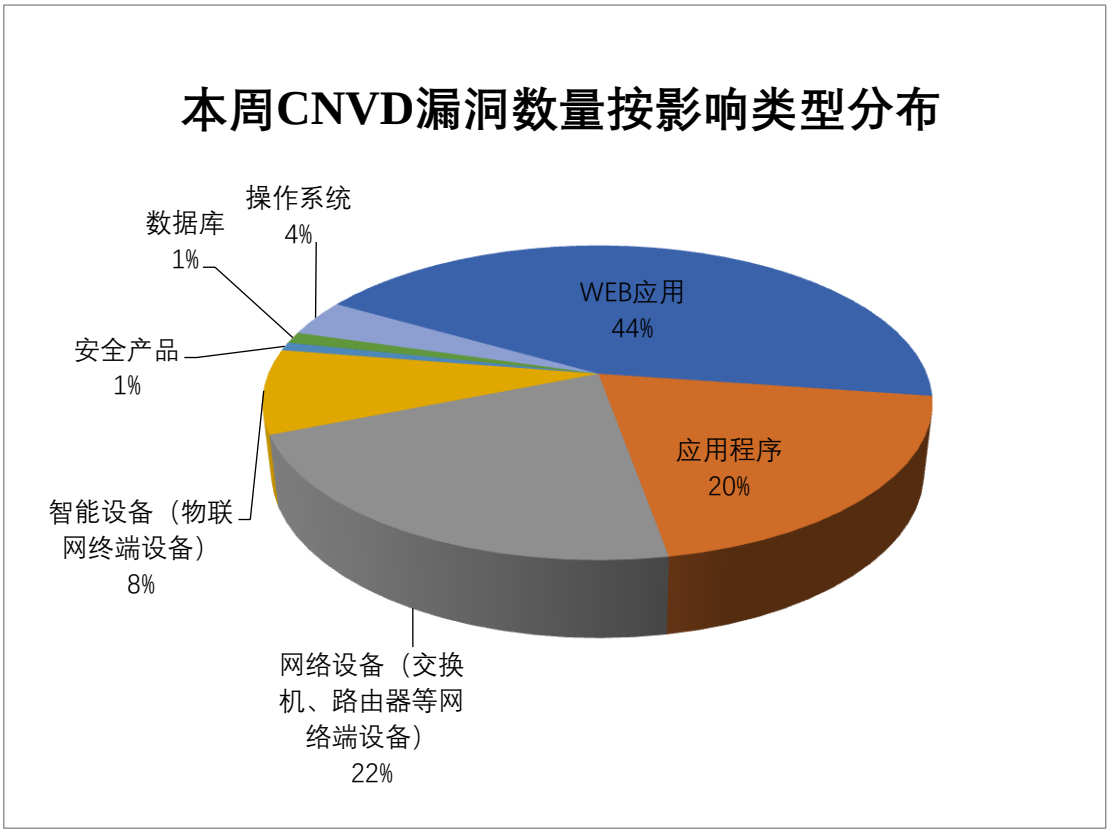

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及友讯电子设备（上海）有限公司、深圳市四海众联网络科技有限公司、新华三技术有限公司等多家厂商的产品，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	友讯电子设备（上海）有限公司	18	5%
2	深圳市四海众联网络科技有限公司	13	4%
3	新华三技术有限公司	13	4%
4	IBM	11	3%
5	Adobe	11	3%
6	Google	9	3%
7	Huawei	9	2%
8	Apache	7	2%
9	Bento4	7	2%
10	其他	248	72%

本周行业漏洞收录情况

本周，CNVD 收录了 64 个电信行业漏洞，20 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Huawei EMUI 和 Magic UI 越界写入漏洞（CNVD-2023-01059）、Google Android 权限提升漏洞（CNVD-2023-01051）、Huawei EMUI 和 Magic UI 拒绝服务漏洞（CNVD-2023-01057）”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/

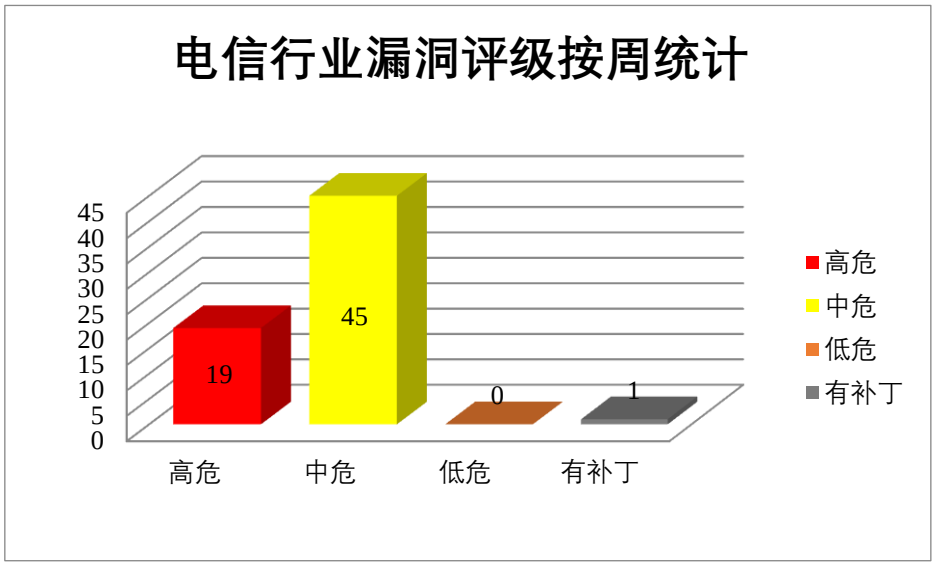

图 3 电信行业漏洞统计

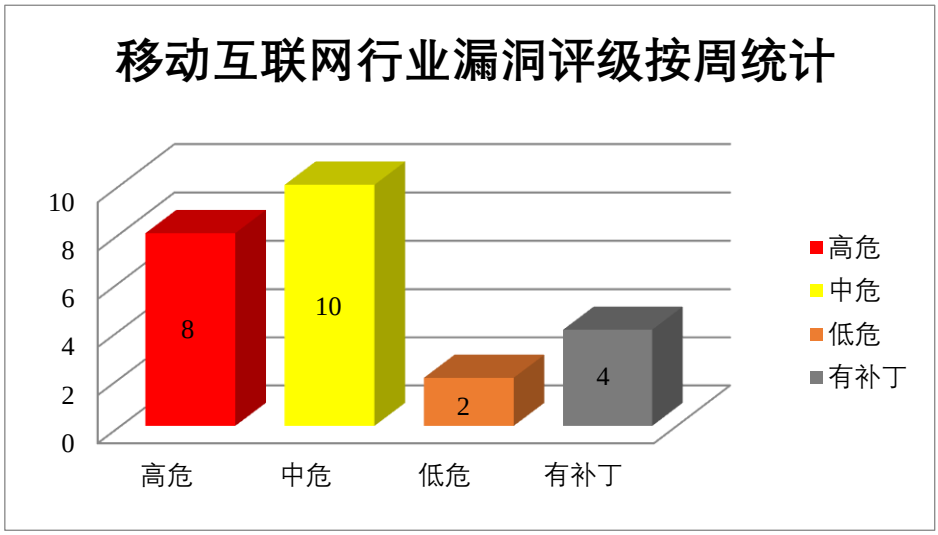

图 4 移动互联网行业漏洞统计

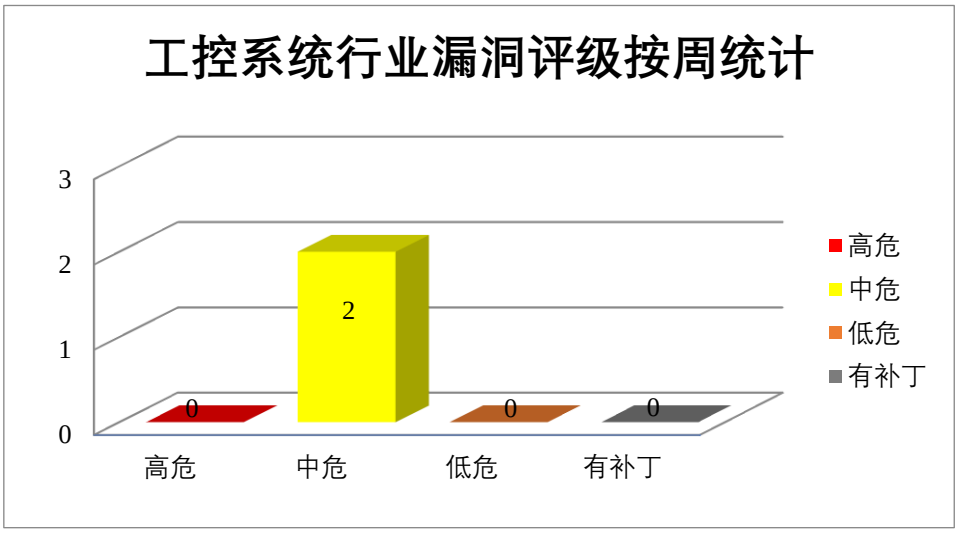

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM AIX 是美国国际商业机器（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。IBM DB2 是美国国际商业机器（IBM）公司的一套关系型数据库管理系统。该系统的执行环境主要有 UNIX、Linux、IBMi、z/OS 以及 Windows 服务器版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行从网站信任的用户传输的恶意和未经授权的操作，通过 AIX SMB 客户端实现拒绝服务等。

CNVD 收录的相关漏洞包括：IBM AIX 拒绝服务漏洞（CNVD-2023-00804、CNVD-2023-00807、CNVD-2023-00806、CNVD-2023-00805、CNVD-2023-00810、CNVD-2023-00809、CNVD-2023-00808）、IBM DB2 跨站请求伪造漏洞（CNVD-2023-00813）。其中，“IBM AIX 权限提升漏洞（CNVD-2023-00805）、IBM DB2 跨站请求伪造漏洞（CNVD-2023-00813）”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-2023-00804

https://www.cnvd.org.cn/flaw/show/CNVD-2023-00807

https://www.cnvd.org.cn/flaw/show/CNVD-2023-00806

https://www.cnvd.org.cn/flaw/show/CNVD-2023-00805

https://www.cnvd.org.cn/flaw/show/CNVD-2023-00810

https://www.cnvd.org.cn/flaw/show/CNVD-2023-00809

https://www.cnvd.org.cn/flaw/show/CNVD-2023-00808

https://www.cnvd.org.cn/flaw/show/CNVD-2023-00813

2、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。Google Pixel 是美国谷歌（Google）公司的一款智能手机。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，获得提升的权限，远程执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-01051）、Google Pixel 缓冲区溢出漏洞（CNVD-2023-01493、CNVD-2023-01492、CNVD-2023-01491、CNVD-2023-01490、CNVD-2023-01494、CNVD-2023-01499、CNVD-2023-01498）。其中，“Google Android 权限提升漏洞（CNVD-2023-01051）、Google Pixel 缓冲区溢出漏洞（CNVD-2023-01492、CNVD-2023-01490）” 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-2023-01051

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01493

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01492

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01491

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01490

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01494

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01499

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01498

3、Huawei 产品安全漏洞

Huawei ws7200-10 是中国华为（HUAWEI）公司的一款无线路由器。Huawei CV81-WDM FW 是中国华为（Huawei）公司的一款激光多功能打印机。Huawei EMUI 是一款基于 Android 开发的移动端操作系统。Huawei Magic UI 是一个智能设备操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过暴力破解获取密码，可能导致系统敏感信息泄露，获得打印机的最高权限，导致服务异常等。

CNVD 收录的相关漏洞包括：Huawei WS7200-10 访问控制错误漏洞、Huawei CV81-WDM FW 输入验证不足漏洞、Huawei CV81-WDM FW 命令注入漏洞、Huawei CV81-WDM FW 输入校验漏洞（CNVD-2023-01056、CNVD-2023-01060）、Huawei EMUI 和 Magic UI 拒绝服务漏洞（CNVD-2023-01057）、Huawei EMUI 和 Huawei Magic UI 越界写入漏洞、Huawei EMUI 和 Magic UI 越界写入漏洞（CNVD-2023-01059）。其中，除“Huawei WS7200-10 访问控制错误漏洞”外其余漏洞的综合评级为“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-2023-01053

https://www.cnvd.org.cn/flaw/show/CNVD-2023-01054
https://www.cnvd.org.cn/flaw/show/CNVD-2023-01055
https://www.cnvd.org.cn/flaw/show/CNVD-2023-01056
https://www.cnvd.org.cn/flaw/show/CNVD-2023-01057
https://www.cnvd.org.cn/flaw/show/CNVD-2023-01058
https://www.cnvd.org.cn/flaw/show/CNVD-2023-01059
https://www.cnvd.org.cn/flaw/show/CNVD-2023-01060

4、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。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞在浏览器上下文中执行恶意 JavaScript。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2023-00009、CNVD-2023-00605、CNVD-2023-00604、CNVD-2023-00603、CNVD-2023-00608、CNVD-2023-00607、CNVD-2023-00606、CNVD-2023-00611）。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-2023-00009
https://www.cnvd.org.cn/flaw/show/CNVD-2023-00605
https://www.cnvd.org.cn/flaw/show/CNVD-2023-00604
https://www.cnvd.org.cn/flaw/show/CNVD-2023-00603
https://www.cnvd.org.cn/flaw/show/CNVD-2023-00608
https://www.cnvd.org.cn/flaw/show/CNVD-2023-00607
https://www.cnvd.org.cn/flaw/show/CNVD-2023-00606
https://www.cnvd.org.cn/flaw/show/CNVD-2023-00611

5、Tenda i22 缓冲区溢出漏洞

Tenda i22 是中国腾达（Tenda）公司的一款无线接入点。本周，Tenda i22 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞提交特殊的请求，可以在系统上下文执行任意代码或者使应用程序崩溃。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-2023-00010

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-2023-00005	phpRedisAdmin 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://github.com/erikdubbelboer/phpRedisAdmin/
CNVD-2023-00805	IBM AIX 权限提升漏洞（CNVD-2023-00805）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ibm.com/support/pages/node/6847947
CNVD-2023-00813	IBM DB2 跨站请求伪造漏洞（CNVD-2023-00813）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ibm.com/support/pages/node/6843071
CNVD-2023-01051	Google Android 权限提升漏洞（CNVD-2023-01051）	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/android-13
CNVD-2023-01054	Huawei CV81-WDM FW 输入验证不足漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20220601-01-66843eb3-en
CNVD-2023-01055	Huawei CV81-WDM FW 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20220601-01-6b47c6b6-cn
CNVD-2023-01056	Huawei CV81-WDM FW 输入校验漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20220608-01-1a91f8a4-cn
CNVD-2023-01057	Huawei EMUI 和 Magic UI 拒绝服务漏洞（CNVD-2023-01057）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://consumer.huawei.com/en/support/bulletin/2022/6/
CNVD-2023-01058	Huawei EMUI 和 Huawei Magic UI 越界写入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://consumer.huawei.com/en/support/bulletin/2022/9/
CNVD-2023-01059	Huawei EMUI 和 Magic UI 越界写入漏洞（CNVD-2023-01059）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://consumer.huawei.com/en/support/bulletin/2022/9/

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞执行从网站信任的

用户传输的恶意和未经授权的操作，通过 AIX SMB 客户端实现拒绝服务等。此外，Google、Huawei、Adobe 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，获得提升的权限，远程执行任意代码等。另外，Tenda i22 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞提交特殊的请求，可以在系统上下文执行任意代码或者使应用程序崩溃。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、Zettlr 输入验证错误漏洞

验证描述

Zettlr 是一款用于专业编辑 Markdown 文件的最全面的编辑器。

Zettlr 2.3.0 版本存在输入验证错误漏洞，该漏洞源于应用程序无 CSP 策略，在渲染 markdown 文件之前未正确验证内容，攻击者可利用该漏洞查看本地的任意文件。

验证信息

POC 链接：https://fluidattacks.com/advisories/avicii/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-01488

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. 流行开发工具 CircleCI 曝出漏洞

开发工具平台 CircleCI 披露发生安全事件，并敦促用户立刻轮换软件项目中的所有“秘密”（存储在项目环境中的敏感信息）。

参考链接：https://www.secrss.com/articles/50792

2. Zoho 敦促修复 ManageEngine 中的一个关键 SQL 注入漏洞

Zoho 正在敦促其客户解决一个 SQL 注入漏洞，漏洞被追踪为 CVE-2022-47523，会影响多个 ManageEngine 产品。

参考链接：https://securityaffairs.com/140369/security/zoho-sql-injection-manageengine.html?_gl=1*rcc3fa*_ga*NjYyNDMxOTU5LjE2MzU5OTc2MDM.*_ga_8ZWTX5HC4Z*MTY3MzAwMzQ1NC45NS4wLjE2NzMwMDM0NTQuMC4wLjA.*_ga_P62M3QN974*MT

Y3MzAwMzQ1NC4yNzQuMC4xNjczMDAzNDU0LjAuMC4w&_ga=2.221244957.464696338.1672970601-662431959.1635997603

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