# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2023 年 11 月 20 日-2023 年 11 月 26 日　　2023 年第 47 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 416 个，其中高危漏洞 191 个、中危漏洞 198 个、低危漏洞 27 个。漏洞平均分值为 6.40。本周收录的漏洞中，涉及 0day 漏洞 363 个（占 87%），其中互联网上出现“WordPress Photo Gallery 跨站脚本漏洞、DevBlog 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 61715 个，与上周（41601 个）环比增加 48%。

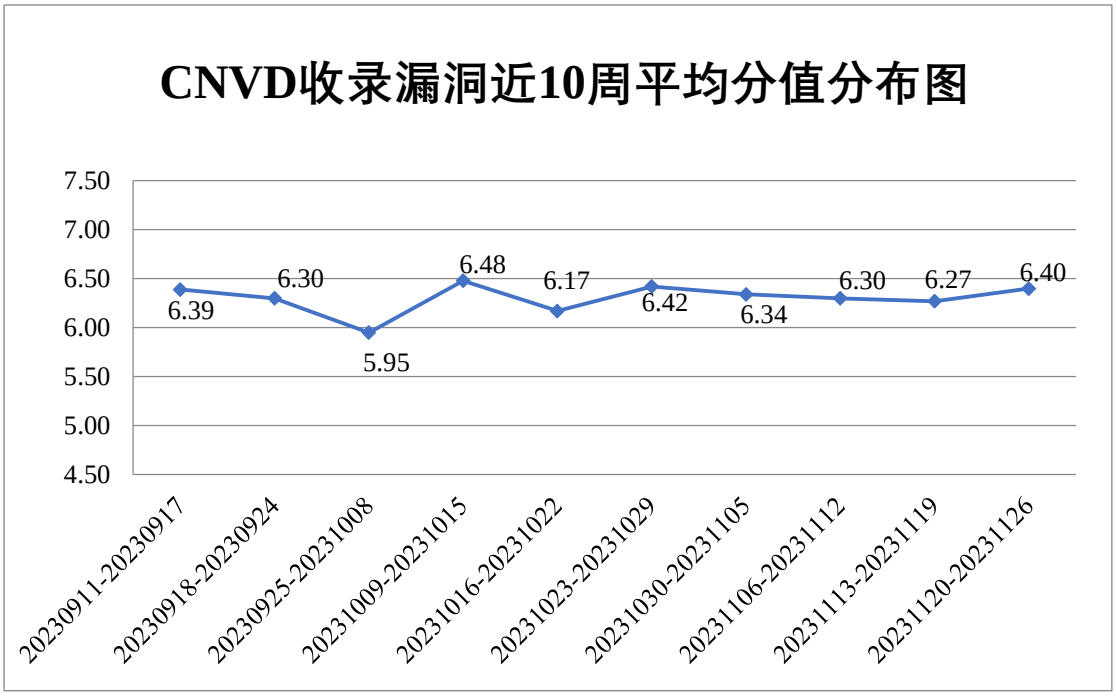


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 23 起，向基础电

信企业通报漏洞事件 18 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 1143 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 210 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 63 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：

友讯电子设备（上海）有限公司、中视购物有限公司、用友网络科技股份有限公司、吉翁电子（深圳）有限公司、北京智联软件技术有限公司、榆林恒生购物中心有限公司、北京中远麒麟科技有限公司、杭州思福迪信息技术有限公司、北京雪迪龙科技股份有限公司、上海茸易科技有限公司、西安交大捷普网络科技有限公司、广州协众软件科技有限公司、武汉鹏达睿智科技有限公司、畅捷通信息技术股份有限公司、东莞市通天星软件科技有限公司、苏州梦图地理信息系统有限责任公司、北京网动网络科技股份有限公司、金蝶软件（中国）有限公司、惠普贸易（上海）有限公司、成都索贝数码科技股份有限公司和百望金赋科技有限公司。

## 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、北京神州绿盟科技有限公司、新华三技术有限公司、天津市国瑞数码安全系统股份有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。亚信科技（成都）有限公司、江苏金盾检测技术股份有限公司、联想集团、河南东方云盾信息技术有限公司、北京山石网科信息技术有限公司、快页信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、贵州多彩网安科技有限公司、杭州海康威视数字技术股份有限公司、湖南泛联新安信息科技有限公司、安徽锋刃信息科技有限公司、广州中科诺泰技术有限公司、内蒙古洞明科技有限公司、赛尔网络有限公司、合肥梆梆信息科技有限公司、杭州默安科技有限公司、北京中关村实验室、上海直画科技有限公司、博智安全科技股份有限公司、山石网科通信技术股份有限公司、中国电信股份有限公司上海研究院、宁夏凯信特信息科技有限公司、安徽天行网安信息安全技术有限公司、河北华测信息技术有限公司、广州安亿信软件科技有限公司、平安银河实验室、北京微步在线科技有限公司、国网山东省电力公司、中国工商银行、中国电信股份有限公司北京研究院、智网安云（武汉）信息技术有限公司、湖北星野科技发展有限公司、杭州中正检测技术有限公司、北京威努特技术有限公司、郑州埃文计算机科技有限公司、江苏金陵科技集团有限公司、北京天防安全科技有限公司、成都安美勤信息技术股份有限公司、信息产业信息安全测评中心、江苏极元信息技术有限公司、浙江东安检测技术有限公司、杭州寻臻科技有限责任公司、南方电网数字电网集团有限公司、山东道普测评技术有限公司、中孚安全技

术有限公司、河北镌远网络科技有限公司及其他个人白帽子向 CNVD 提交了 61715 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和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 57261 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） | 37975 | 37975 |
| 奇安信网神（补天平台） | 18955 | 18955 |
| 北京天融信网络安全技术有限公司 | 953 | 24 |
| 北京神州绿盟科技有限公司 | 847 | 338 |
| 新华三技术有限公司 | 609 | 1 |
| 天津市国瑞数码安全系统股份有限公司 | 471 | 0 |
| 三六零数字安全科技集团有限公司 | 331 | 331 |
| 北京数字观星科技有限公司 | 322 | 0 |
| 深信服科技股份有限公司 | 258 | 0 |
| 阿里云计算有限公司 | 159 | 8 |
| 北京启明星辰信息安全技术有限公司 | 128 | 39 |
| 杭州安恒信息技术股份有限公司 | 89 | 5 |
| 北京知道创宇信息技术有限公司 | 89 | 5 |
| 安天科技集团股份有限公司 | 60 | 0 |
| 北京升鑫网络科技有限公司（青藤云） | 32 | 32 |
| 中电科网络安全科技股份有限公司 | 29 | 10 |

| | | |
|---|---|---|
| 北京长亭科技有限公司 | 21 | 1 |
| 杭州迪普科技股份有限公司 | 20 | 0 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 12 | 12 |
| 京东科技信息技术有限公司 | 11 | 11 |
| 南京联成科技发展股份有限公司 | 11 | 11 |
| 浙江大华技术股份有限公司 | 2 | 2 |
| 华为技术有限公司 | 1 | 1 |
| 亚信科技（成都）有限公司 | 1817 | 1817 |
| 江苏金盾检测技术股份有限公司 | 34 | 34 |
| 联想集团 | 23 | 23 |
| 河南东方云盾信息技术有限公司 | 23 | 23 |
| 北京山石网科信息技术有限公司 | 23 | 23 |
| 快页信息技术有限公司 | 20 | 20 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 14 | 14 |
| 贵州多彩网安科技有限公司 | 13 | 13 |
| 杭州海康威视数字技术股份有限公司 | 12 | 12 |
| 湖南泛联新安信息科技有限公司 | 9 | 9 |
| 安徽锋刃信息科技有 | 7 | 7 |

| | | |
|---|---|---|
| 限公司 | | |
| 广州中科诺泰技术有限公司 | 6 | 6 |
| 内蒙古洞明科技有限公司 | 5 | 5 |
| 赛尔网络有限公司 | 4 | 4 |
| 合肥梆梆信息科技有限公司 | 3 | 3 |
| 杭州默安科技有限公司 | 3 | 3 |
| 北京中关村实验室 | 3 | 3 |
| 上海直画科技有限公司 | 3 | 3 |
| 博智安全科技股份有限公司 | 3 | 3 |
| 山石网科通信技术股份有限公司 | 3 | 3 |
| 中国电信股份有限公司上海研究院 | 3 | 3 |
| 宁夏凯信特信息科技有限公司 | 2 | 2 |
| 安徽天行网安信息安全技术有限公司 | 2 | 2 |
| 河北华测信息技术有限公司 | 2 | 2 |
| 广州安亿信软件科技有限公司 | 2 | 2 |
| 平安银河实验室 | 2 | 2 |
| 北京微步在线科技有限公司 | 2 | 2 |
| 国网山东省电力公司 | 2 | 2 |
| 中国工商银行 | 1 | 1 |
| 中国电信股份有限公司北京研究院 | 1 | 1 |
| 智网安云（武汉）信 | 1 | 1 |

| | | |
|---|---|---|
| 息技术有限公司 | | |
| 湖北星野科技发展有限公司 | 1 | 1 |
| 杭州中正检测技术有限公司 | 1 | 1 |
| 北京威努特技术有限公司 | 1 | 1 |
| 郑州埃文计算机科技有限公司 | 1 | 1 |
| 江苏金陵科技集团有限公司 | 1 | 1 |
| 北京天防安全科技有限公司 | 1 | 1 |
| 成都安美勤信息技术股份有限公司 | 1 | 1 |
| 信息产业信息安全测评中心 | 1 | 1 |
| 江苏极元信息技术有限公司 | 1 | 1 |
| 浙江东安检测技术有限公司 | 1 | 1 |
| 杭州寻臻科技有限责任公司 | 1 | 1 |
| 南方电网数字电网集团有限公司 | 1 | 1 |
| 山东道普测评技术有限公司 | 1 | 1 |
| 中孚安全技术有限公司 | 1 | 1 |
| 河北镌远网络科技有限公司 | 1 | 1 |
| CNCERT 广西分中心 | 3 | 3 |
| 个人 | 1888 | 1888 |
| 报送总计 | 65339 | 61715 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 416 个漏洞。WEB 应用 224 个，应用程序 87 个，网络设备（交换机、路由器等网络端设备）64 个，智能设备（物联网终端设备）19 个，操作系统 13 个，安全产品 5 个，数据库 4 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 | 224 |
| 应用程序 | 87 |
| 网络设备（交换机、路由器等网络端设备） | 64 |
| 智能设备（物联网终端设备） | 19 |
| 操作系统 | 13 |
| 安全产品 | 5 |
| 数据库 | 4 |

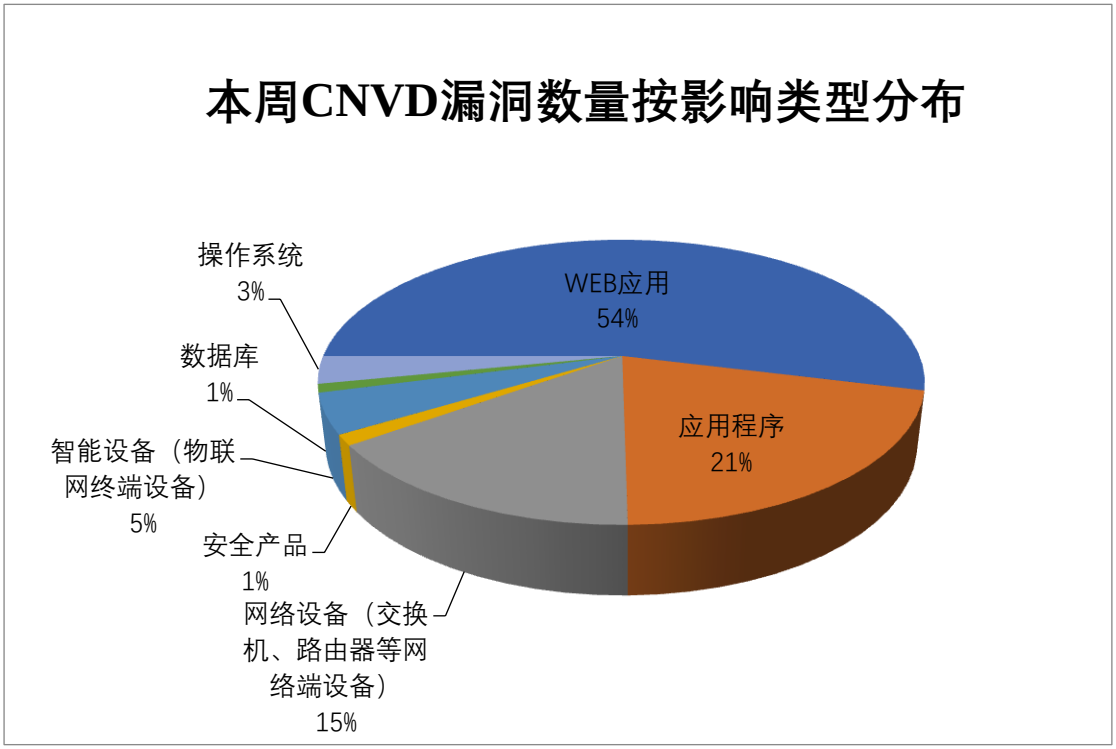


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及北京星网锐捷网络技术有限公司、北京百卓网络技术有限公司、用友网络科技股份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 | 北京星网锐捷网络技术有限公司 | 20 | 5% |
| 2 | 北京百卓网络技术有限公司 | 19 | 5% |
| 3 | 用友网络科技股份有限公司 | 15 | 4% |
| 4 | Adobe | 12 | 3% |
| 5 | Huawei | 10 | 2% |
| 6 | Apache | 10 | 2% |
| 7 | FreeImage | 10 | 2% |
| 8 | 爱普生（中国）有限公司 | 9 | 2% |
| 9 | IBM | 8 | 2% |
| 10 | 其他 | 303 | 73% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 39 个电信行业漏洞，23 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 HarmonyOS 和 EMUI 拒绝服务漏洞（CNVD-2023-88961）、Rockwell Automation ThinManager ThinServer 拒绝服务漏洞”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/

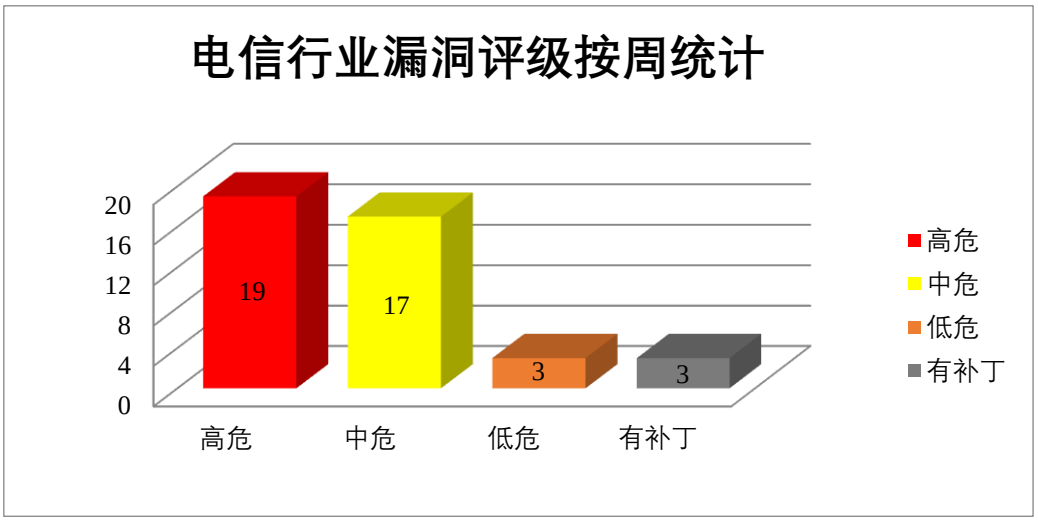


图 3 电信行业漏洞统计

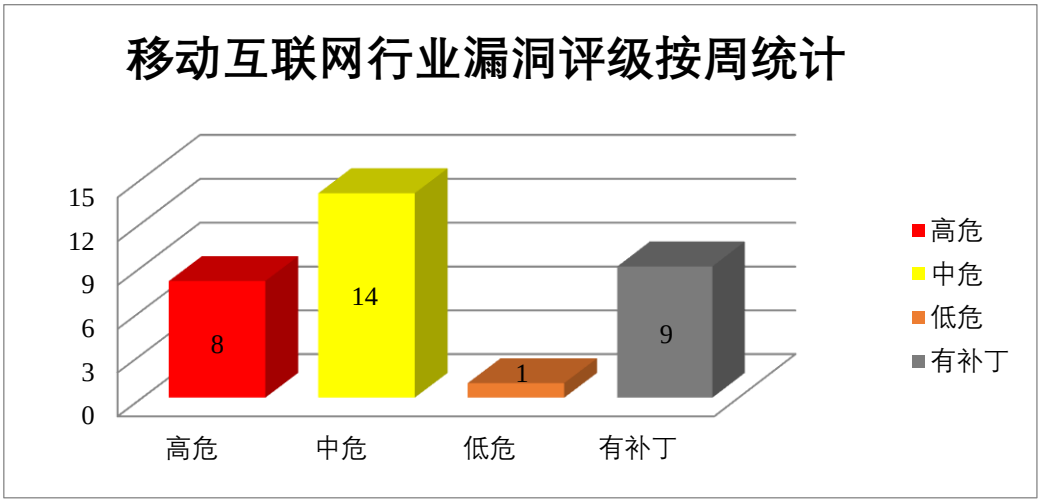


图 4 移动互联网行业漏洞统计

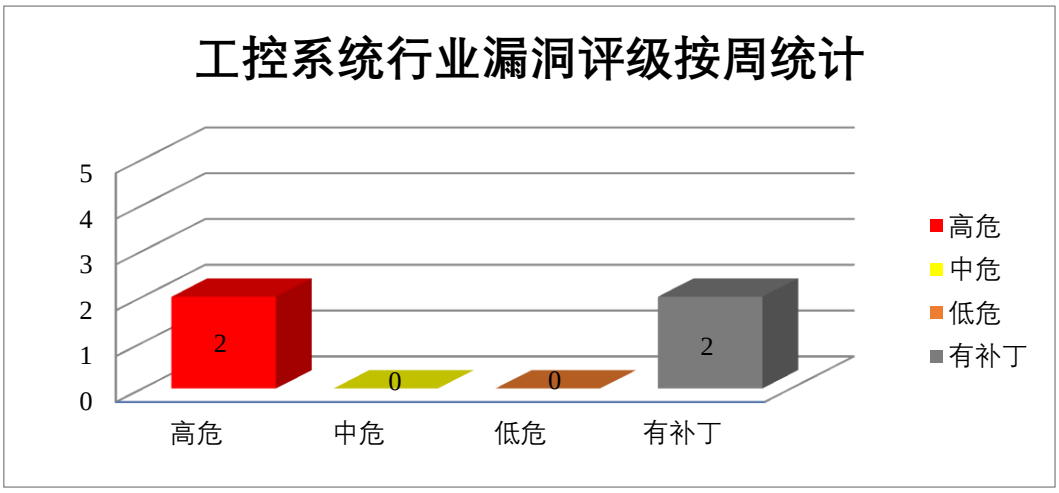


图 5 工控系统行业漏洞统计

## 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 Audition 是美国奥多比（Adobe）公司的一套多音轨编辑工具。该产品主要使用包含多音轨、波形和光谱显示的完善工具集对音频内容进行混音、编辑和创建等。Adobe Media Encoder 是一款音、视频编码应用程序。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代码，导致敏感内存泄露。

CNVD 收录的相关漏洞包括：Adobe Audition 越界读取漏洞（CNVD-2023-88380、CNVD-2023-88658、CNVD-2023-88659）、Adobe Audition 越界写入漏洞（CNVD-2023-88381）、Adobe Audition 堆缓冲区溢出漏洞、Adobe Audition 未初始化指针访问漏洞（CNVD-2023-88656、CNVD-2023-88660）、Adobe Media Encoder 越界写入漏洞（CNVD-2023-88662）。其中，除“Adobe Audition 未初始化指针访问漏洞（CNVD-2023-88660）”外，其余的综合评级为“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-2023-88380

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88381

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88655

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88656

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88658

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88659

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88660

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88662

### 2、 Apache 产品安全漏洞

Apache Airflow 是美国阿帕奇（Apache）基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。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，在系统上执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Apache Airflow Google Provider 输入验证错误漏洞（CNVD-2023-88040、CNVD-2023-88041）、Apache Airflow Hive Provider 代码注入漏洞、Apache Airflow 权限提升漏洞、Apache Airflow 安全绕过漏洞、Apache Airflow AWS Provider 信息泄露漏洞、Apache Airflow Sqoop Provider 输入验证错误漏洞、Apache Airflow Hive Provider 输入验证错误漏洞。其中，除“Apache Airflow 安全绕过漏洞”外，其余的综合评级为“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-2023-88040

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88039

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88038

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88037

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88044

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88043

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88042

https://www.cnvd.org.cn/flaw/show/CNVD-2023-88041

### 3、 Huawei 产品安全漏洞

Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。Huawei EMUI 是华为公司开发的一种基于 Android 操作系统的用户界面。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，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei HarmonyOS 和 EMUI 权限管理漏洞、Huawei HarmonyOS 和 EMUI 越界写入漏洞、Huawei HarmonyOS 和 EMUI 权限控制漏洞（C

NVD-2023-88957）、Huawei HarmonyOS 信息泄露漏洞（CNVD-2023-88958）、Huawei HarmonyOS 和 EMUI 信息泄露漏洞（CNVD-2023-88960、CNVD-2023-88962）、Huawei HarmonyOS 和 EMUI 越界访问漏洞、Huawei HarmonyOS 和 EMUI 内存错误引用洞。其中，除“Huawei HarmonyOS 和 EMUI 权限控制漏洞（CNVD-2023-88957）”外，其余的综合评级为“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-2023-88955
https://www.cnvd.org.cn/flaw/show/CNVD-2023-88956
https://www.cnvd.org.cn/flaw/show/CNVD-2023-88957
https://www.cnvd.org.cn/flaw/show/CNVD-2023-88958
https://www.cnvd.org.cn/flaw/show/CNVD-2023-88960
https://www.cnvd.org.cn/flaw/show/CNVD-2023-88962
https://www.cnvd.org.cn/flaw/show/CNVD-2023-88963
https://www.cnvd.org.cn/flaw/show/CNVD-2023-88966

### 4、IBM 产品安全漏洞

IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从日志文件中获取敏感信息，在系统上执行任意命令等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 跨站请求伪造漏洞（CNVD-2023-91223）、IBM InfoSphere Information Server CSV 注入漏洞（CNVD-2023-91222）、IBM InfoSphere Information Server 权限提升漏洞（CNVD-2023-91221）、IBM InfoSphere Information Server 目录遍历漏洞、IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2023-91225、CNVD-2023-91224、CNVD-2023-91227）、IBM InfoSphere Information Server 拒绝服务漏洞（CNVD-2023-91228）。其中，“IBM InfoSphere Information Server 权限提升漏洞（CNVD-2023-91221）、IBM InfoSphere Information Server 目录遍历漏洞、IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2023-91224）”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-2023-91223
https://www.cnvd.org.cn/flaw/show/CNVD-2023-91222
https://www.cnvd.org.cn/flaw/show/CNVD-2023-91221
https://www.cnvd.org.cn/flaw/show/CNVD-2023-91227
https://www.cnvd.org.cn/flaw/show/CNVD-2023-91226
https://www.cnvd.org.cn/flaw/show/CNVD-2023-91225
https://www.cnvd.org.cn/flaw/show/CNVD-2023-91224

https://www.cnvd.org.cn/flaw/show/CNVD-2023-91228

### 5、TOTOLINK A3700R 命令执行漏洞

TOTOLINK A3700R 是中国吉翁电子（TOTOLINK）公司的一款无线路由器。本周，TOTOLINK A3700R 被披露存在命令执行漏洞。攻击者可利用该漏洞通过 UploadFirmwareFile 函数的 FileName 参数执行任意代码。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-2023-91230

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-2023-88039 | Apache Airflow Hive Provider 代码注入漏洞 | 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/dl20xxd51xvlx0zzc0wzgxfjwgtbbxo3 |
| CNVD-2023-88380 | Adobe Audition 越界读取漏洞（CNVD-2023-88380） | 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/audition/apsb23-64.html |
| CNVD-2023-88655 | Adobe Audition 堆缓冲区溢出漏洞 | 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/audition/apsb23-64.html |
| CNVD-2023-88658 | Adobe Audition 越界读取漏洞（CNVD-2023-88658） | 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/audition/apsb23-64.html |
| CNVD-2023-88955 | Huawei HarmonyOS 和 EMUI 权限管理漏洞 | 高 | 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://consumer.huawei.com/cn/support/bulletin/2023/11/ |
| CNVD-2023-88956 | Huawei HarmonyOS 和 EMUI 越界写入漏洞 | 高 | 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://consumer.huawei.com/cn/support/bulletin/2023/11/ |
| CNVD-2023-88963 | Huawei HarmonyOS 和 EMUI 越界访问漏洞 | 高 | 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： |

| | | | |
|---|---|---|---|
| | | | https://consumer.huawei.com/cn/support/bulletin/2023/11/ |
| CNVD-2023-91226 | IBM InfoSphere Information Server 目录遍历漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/6953521 |
| CNVD-2023-91235 | Rockwell Automation ThinManager ThinServer 输入验证错误漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.myscada.org/download/#mypro |
| CNVD-2023-91548 | OpenHarmony 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://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2023/2023-12.md |

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代码，导致敏感内存泄露。此外，Apache、Huawei、IBM 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，在系统上执行任意代码，导致拒绝服务等。另外，TOTOLINK A3700R 被披露存在命令执行漏洞。攻击者可利用漏洞通过 UploadFirmwareFile 函数的 FileName 参数执行任意代码。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、DevBlog 跨站脚本漏洞

**验证描述**

DevBlog 是 Arman Idrisi 个人开发者的一个使用 Node.js (Express) 和 MongoDB 开发的博客项目。

DevBlog v1.0 版本存在跨站脚本漏洞，该漏洞源于应用对上传的文件缺少有效的验证，攻击者可利用该漏洞上传恶意 HTML 文件。

**验证信息**

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

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-91232

**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. ownCloud 文件共享程序中曝出三个安全漏洞

开源文件共享软件 ownCloud 近日警告称存在三个安全漏洞，其中一个漏洞可能会暴漏管理员密码和邮件服务器凭证。

参考链接：https://www.freebuf.com/news/384893.html

### 2. 指纹传感器漏洞可让攻击者绕过 Windows Hello 登录

一项新的研究发现了多个漏洞，这些漏洞可用于绕过戴尔 Inspiron 灵越 15、联想 ThinkPad T14 和 Microsoft Surface Pro X 笔记本电脑上的 Windows Hello 身份验证。

参考链接：http://www.anquan419.com/knews/24/6322.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