# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2023 年 05 月 15 日-2023 年 05 月 21 日** **2023 年第 20 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 483 个，其中高危漏洞 230 个、中危漏洞 224 个、低危漏洞 29 个。漏洞平均分值为 6.43。本周收录的漏洞中，涉及 0day 漏洞 428 个（占 89%），其中互联网上出现“Vehicle Booking System 文件上传漏洞、SIYUCMS 远程代码执行漏洞”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 15110 个，与上周（4646 个）环比增加 2.25 倍。

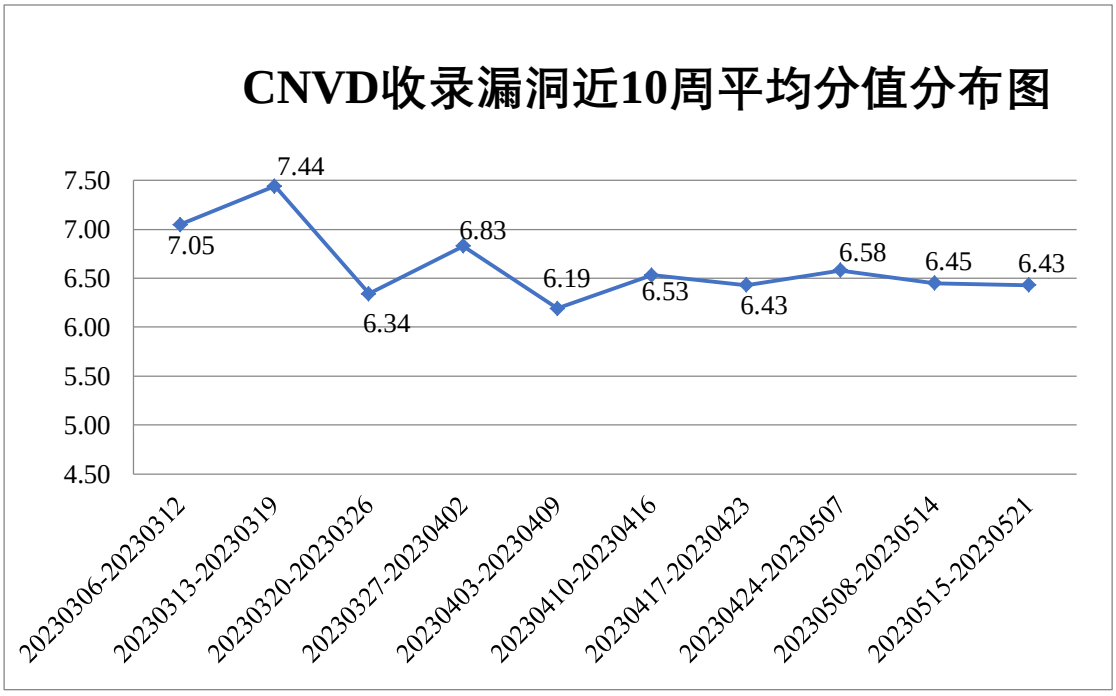


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 25 起，向基础电

信企业通报漏洞事件 34 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 1961 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 357 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 87 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：

卓想云创科技集团有限公司、卓豪（中国）技术有限公司、珠海玖时光科技有限公司、中能易电新能源技术有限公司、中科数字通（北京）科技有限公司、中金亚洲（北京）国际互联网科技有限公司、正奇晟业（北京）科技有限公司、浙江中易慧能科技有限公司、浙江五京科技集团有限公司、浙江同花顺网络科技有限公司、浙江名课文化艺术有限公司、浙江多典智能科技集团有限公司、长沙市同迅计算机科技有限公司、长沙米拓信息技术有限公司、长城汽车股份有限公司、云南力诺科技有限公司、云南滇约出行科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、义乌中国小商品城大数据有限公司、西安知先信息技术有限公司、西安瑞友信息技术资讯有限公司、西安必应人力资源管理有限公司、武汉金同方科技有限公司、武汉达梦数据库有限公司、网易有道信息技术（北京）有限公司、天津天堰科技股份有限公司、天地（常州）自动化股份有限公司、泰华智慧产业集团股份有限公司、台达电子企业管理（上海）有限公司、宿迁鑫潮信息技术有限公司、苏州元速信息技术有限公司、四平市九州易通科技有限公司、深圳拓安信物联股份有限公司、深圳市英威腾电气股份有限公司、深圳市亿图软件有限公司、深圳市前海弘毅华浩投资有限公司、深圳市明源云科技有限公司、深圳市吉祥腾达科技有限公司、深圳市华德安科技有限公司、深圳市宏电技术股份有限公司、深圳市福尔科技有限公司、深圳市道尔智控科技股份有限公司、深圳市博思高科技有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海宜同贸易有限公司、上海新华控制技术集团科技有限公司、上海良栀之志网络科技有限公司、上海徽行供应链有限公司、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、上海多维度网络科技股份有限公司、上海博达数据通信有限公司、上海百奇网络信息技术有限公司、上海阿法迪智能数字科技股份有限公司、熵基科技股份有限公司、山西联运集团股份有限公司、山东中创软件商用中间件股份有限公司、山东力创科技股份有限公司、厦门优胜卫厨科技有限公司、厦门四信通信科技有限公司、厦门市理臣教育服务有限公司、厦门凤凰创壹软件有限公司、赛博爱思（上海）软件有限公司、瑞斯康达、青岛易软天创、青岛迅博信息技术有限公司、青岛培诺教育科技股份有限公司、普宙科技有限公司、普联技术有限公司、南宁迈世信息技术有限公司、迈普通信技术股份有限公司、力合科技（湖南）股份有限公司、浪潮通用软件有限公司、朗坤智慧科技股份有限公司、昆明奥远科技有限公司、敬业钢铁有限公司、金蝶软件（中国）有限公司、江西金磊科技发展有限公司、江苏汇文软件有限公司、江苏邦宁科技有限公司、济南卓源

软件有限公司、吉翁电子（深圳）有限公司、慧与（中国）有限公司、湖南强智科技发展有限公司、湖南快乐车行露营地投资发展有限公司、湖北知音传媒股份有限公司、杭州中宝科技有限公司、杭州予尚网络科技有限公司、杭州先锋电子技术股份有限公司、杭州飞致云信息科技有限公司、杭州藏茗山科技有限公司、广州中望龙腾软件股份有限公司、广州市非客网络科技有限公司、广州极电通信技术有限公司、广西车便捷数字科技股份有限公司、广联达科技股份有限公司、广东宜教通教育有限公司、福建淘汽互联科技有限公司、帆软软件有限公司、东华医为科技有限公司、帝国软件、成都英孚克斯科技有限公司、成都行行行科技有限公司、成都索贝数码科技股份有限公司、成都生动网络科技有限公司、成都锦宏商务旅游汽车租赁有限公司、成都飞鱼星科技股份有限公司、车车保险销售服务有限公司、常州伟泰科技股份有限公司、北京子在川上科技有限公司、北京中远麒麟科技有限公司、北京中科美伦医疗股份有限公司、北京致远互联软件股份有限公司、北京臻鼎科技有限公司、北京意园创新办公服务股份有限公司、北京亿思摩博网络科技有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京网康科技有限公司、北京通达信科科技有限公司、北京市公交汽车驾驶学校有限公司、北京三快科技有限公司、北京人大金仓信息技术股份有限公司、北京欧倍尔软件技术开发有限公司、北京凯特伟业科技有限公司、北京居然智慧家智能科技有限公司、北京九思协同软件有限公司、北京竞业达数码科技股份有限公司、北京金和网络股份有限公司、北京宏达一甲教育科技有限公司、北京和利时集团、北京好雨科技有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、宝利通公司、奥琦玮信息科技（北京）有限公司、安徽皖通邮电股份有限公司、SEMCMS、mymps、jeewms 和 DocCms X 开发团队。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、新华三技术有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、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。快页信息技术有限公司、上海齐同信息科技有限公司、联想集团、北京升鑫网络科技有限公司、重庆电信系统集成公司、安徽锋刃信息科技有限公司、河南信安世纪科技有限公司、杭州美创科技有限公司、河南东方云盾信息技术有限公司、内蒙古洞明科技有限公司、湖南轻山信息技术有限公司、广州安亿信软件科技有限公司、中孚安全技术有限公司、赛尔网络有限公司、北京华云安信息技术有限公司、河北锐远网络科技有限公司、北京时代新威信息技术有限公司、北京山石网科信息技术有限公司、北京君云天下科技有限公司、任子行网络技术股份有限公司、北京六方云信息技术有限公司、福建省海峡信息技术有限公司、北京安帝科技有限公司、上海嘉韦思信息技术有限公司、北京微步在线科技有限公司、河南灵创电子

科技有限公司、重庆易阅科技有限公司、华泰证券股份有限公司、超聚变数字技术有限公司、神州灵云（北京）科技有限公司、海南神州希望网络有限公司及其他个人白帽子向 CNVD 提交了 15110 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）、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 12266 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） | 9637 | 9637 |
| 斗象科技（漏洞盒子） | 1231 | 1231 |
| 三六零数字安全科技集团有限公司 | 1101 | 1101 |
| 北京启明星辰信息安全技术有限公司 | 1053 | 16 |
| 新华三技术有限公司 | 659 | 0 |
| 深信服科技股份有限公司 | 557 | 5 |
| 上海交大 | 297 | 297 |
| 北京神州绿盟科技有限公司 | 267 | 0 |
| 安天科技集团股份有限公司 | 211 | 0 |
| 阿里云计算有限公司 | 169 | 0 |
| 北京天融信网络安全技术有限公司 | 161 | 1 |
| 北京数字观星科技有限公司 | 104 | 0 |
| 天津市国瑞数码安全系统股份有限公司 | 59 | 0 |
| 北京长亭科技有限公司 | 29 | 1 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 18 | 18 |
| 杭州迪普科技股份有 | 16 | 2 |

| | | |
|---|---|---|
| 限公司 | | |
| 中国电信集团系统集成有限责任公司 | 16 | 0 |
| 杭州安恒信息技术股份有限公司 | 10 | 10 |
| 浙江大华技术股份有限公司 | 3 | 3 |
| 北京知道创宇信息技术股份有限公司 | 3 | 0 |
| 华为技术有限公司 | 2 | 2 |
| 南京众智维信息科技有限公司 | 1 | 1 |
| 快页信息技术有限公司 | 621 | 621 |
| 上海齐同信息科技有限公司 | 90 | 90 |
| 联想集团 | 55 | 55 |
| 北京升鑫网络科技有限公司 | 41 | 41 |
| 重庆电信系统集成公司 | 38 | 38 |
| 安徽锋刃信息科技有限公司 | 34 | 34 |
| 河南信安世纪科技有限公司 | 20 | 20 |
| 杭州美创科技有限公司 | 18 | 18 |
| 河南东方云盾信息技术有限公司 | 15 | 15 |
| 内蒙古洞明科技有限公司 | 12 | 12 |
| 湖南轻山信息技术有限公司 | 8 | 8 |
| 广州安亿信软件科技有限公司 | 5 | 5 |

| | | |
|---|---|---|
| 中孚安全技术有限公司 | 5 | 5 |
| 赛尔网络有限公司 | 4 | 4 |
| 北京华云安信息技术有限公司 | 3 | 3 |
| 河北镌远网络科技有限公司 | 3 | 3 |
| 北京时代新威信息技术有限公司 | 3 | 3 |
| 北京山石网科信息技术有限公司 | 3 | 3 |
| 北京君云天下科技有限公司 | 3 | 3 |
| 任子行网络技术股份有限公司 | 2 | 2 |
| 北京六方云信息技术有限公司 | 2 | 2 |
| 福建省海峡信息技术有限公司 | 2 | 2 |
| 北京安帝科技有限公司 | 2 | 2 |
| 上海嘉韦思信息技术有限公司 | 2 | 2 |
| 北京微步在线科技有限公司 | 1 | 1 |
| 河南灵创电子科技有限公司 | 1 | 1 |
| 重庆易阅科技有限公司 | 1 | 1 |
| 华泰证券股份有限公司 | 1 | 1 |
| 超聚变数字技术有限公司 | 1 | 1 |
| 神州灵云（北京）科技有限公司 | 1 | 1 |

| | | |
|---|---|---|
| 海南神州希望网络有限公司 | 1 | 1 |
| CNCERT 贵州分中心 | 2 | 2 |
| CNCERT 河北分中心 | 1 | 1 |
| 个人 | 1784 | 1784 |
| 报送总计 | 18389 | 15110 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 483 个漏洞。WEB 应用 299 个，应用程序 121 个，网络设备（交换机、路由器等网络端设备）34 个，智能设备（物联网终端设备）15 个，操作系统 8 个，安全产品 4 个，区块链外围系统 2 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 | 299 |
| 应用程序 | 121 |
| 网络设备（交换机、路由器等网络端设备） | 34 |
| 智能设备（物联网终端设备） | 15 |
| 操作系统 | 8 |
| 安全产品 | 4 |
| 区块链外围系统 | 2 |

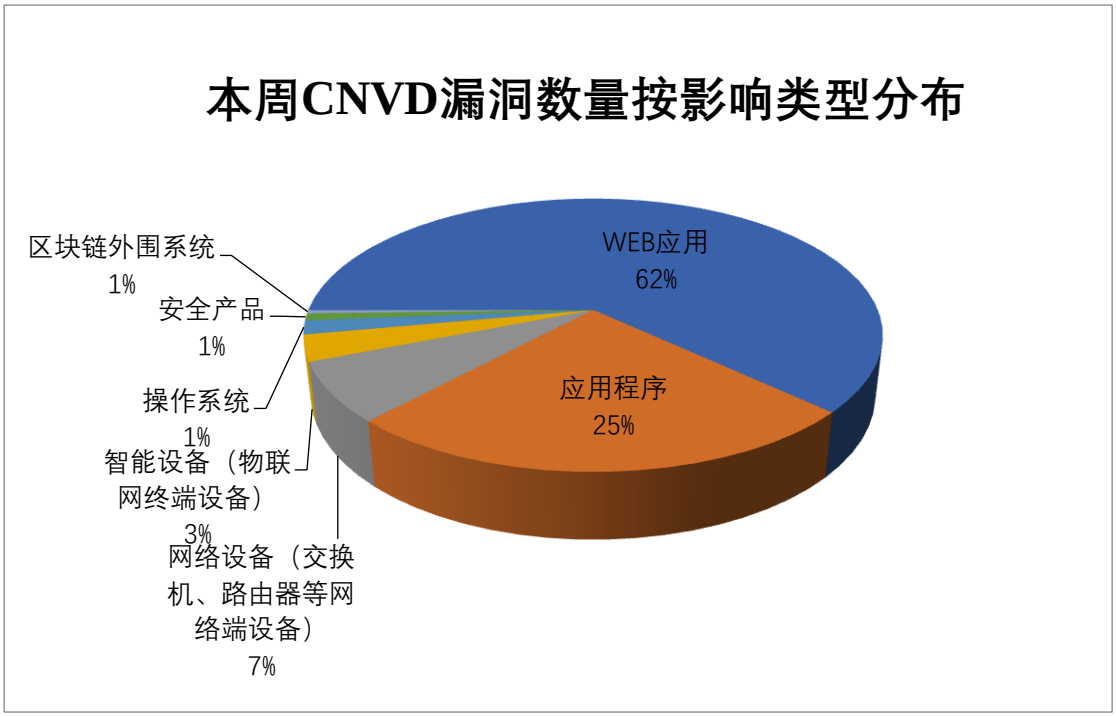

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SEMCMS、Huawei、IBM 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 | SEMCMS | 15 | 3% |
| 2 | Huawei | 13 | 3% |
| 3 | IBM | 11 | 2% |
| 4 | Schneider Electric | 11 | 2% |
| 5 | 商派软件有限公司 | 11 | 2% |
| 6 | FunAdmin | 10 | 2% |
| 7 | Adobe | 8 | 2% |
| 8 | Campcodes | 8 | 2% |
| 9 | Carlo Montero | 7 | 1% |
| 10 | 其他 | 389 | 81% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 26 个电信行业漏洞，52 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，“ZTE MF297D 信息泄露漏洞、mySCADA myPRO 操作系统命令注入漏洞（CNVD-2023-38196）”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/

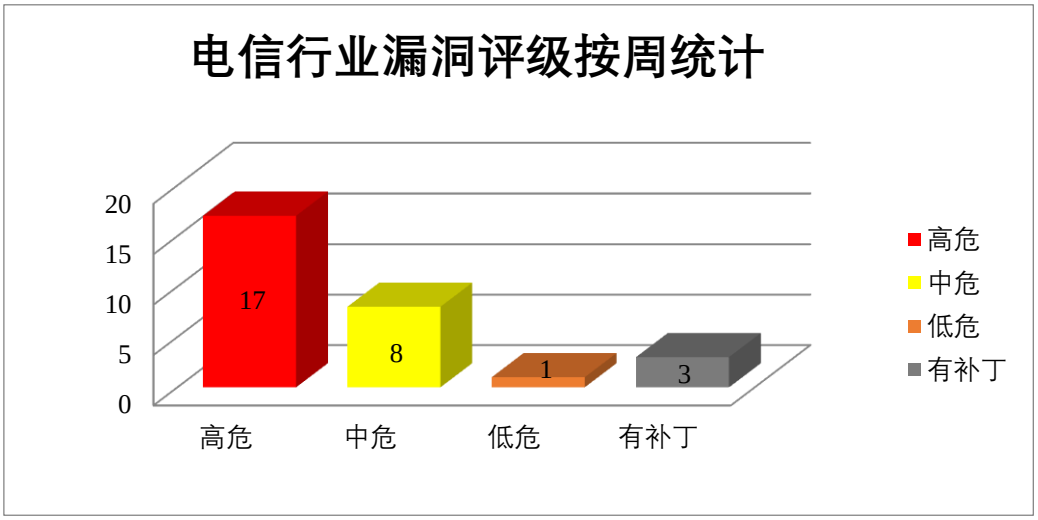


图 3 电信行业漏洞统计

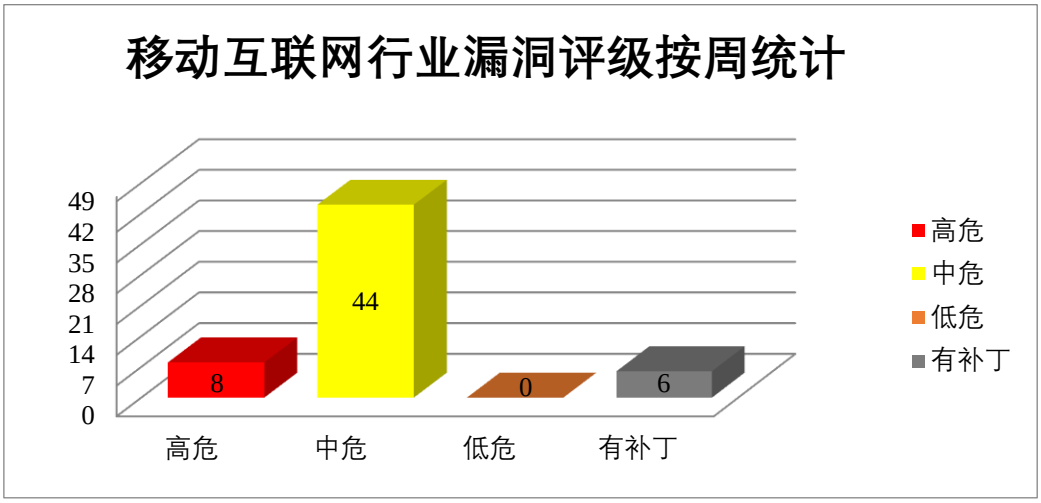


图 4 移动互联网行业漏洞统计

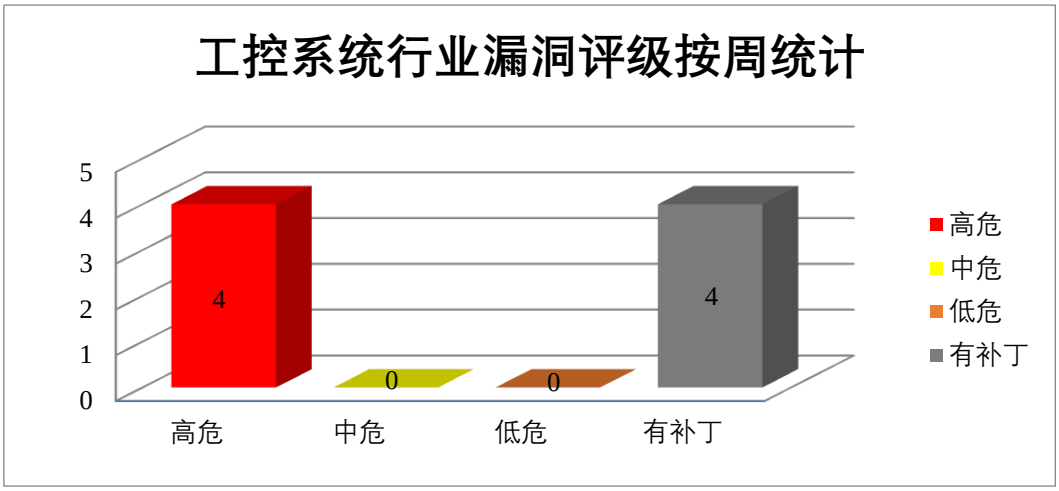


图 5 工控系统行业漏洞统计

## 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、Huawei 产品安全漏洞

Huawei HiLink AI Life 是中国华为（Huawei）公司的全屋智能解决方案。Huawei EMUI 是一款基于 Android 开发的移动端操作系统。Huawei HarmonyOS 是提供一个基于微内核的全场景分布式操作系统。Huawei BiSheng-WNM FW 是一款华为打印机。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信息，导致恶意隐藏应用程序图标，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei HiLink AI Life 授权问题漏洞、Huawei EMUI 和 HarmonyOS 拒绝服务漏洞（CNVD-2023-38960）、Huawei EMUI 和 HarmonyOS 信息泄露漏洞、Huawei EMUI 和 HarmonyOS 安全绕过漏洞、Huawei EMUI 和 HarmonyOS 双重释放漏洞、Huawei BiSheng-WNM FW 拒绝服务漏洞（CNVD-2023-39039、CNVD-2023-39041、CNVD-2023-39040）。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-2023-37156
https://www.cnvd.org.cn/flaw/show/CNVD-2023-38960
https://www.cnvd.org.cn/flaw/show/CNVD-2023-38962
https://www.cnvd.org.cn/flaw/show/CNVD-2023-38961
https://www.cnvd.org.cn/flaw/show/CNVD-2023-38964
https://www.cnvd.org.cn/flaw/show/CNVD-2023-39039
https://www.cnvd.org.cn/flaw/show/CNVD-2023-39041
https://www.cnvd.org.cn/flaw/show/CNVD-2023-39040

### 2、 Schneider Electric 产品安全漏洞

Schneider Electric StruxureWare Data Center Expert 是法国施耐德电气（Schneider Electric）公司的一种监控软件。适用于各种组织监控其全公司范围内的电力、制冷、安全、环境。Schneider Electric Igss Data Server 是一个交互式图形 Scada 系统的数据服务器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发送特制的消息来获取操作和读取 IGSS 项目报告目录中的文件，导致远程代码执行等。

CNVD 收录的相关漏洞包括：Schneider Electric StruxureWare Data Center Expert 操作系统命令注入漏洞、Schneider Electric StruxureWare Data Center Expert 访问控制错误漏洞（CNVD-2023-37594）、Schneider Electric StruxureWare Data Center Expert 访问控制错误漏洞（CNVD-2023-37593、CNVD-2023-37592）、Schneider Electric StruxureWare Data Center Expert 代码注入漏洞（CNVD-2023-37598、CNVD-2023-37597）、Schneider Electric IGSS Data Server 缓冲区溢出漏洞（CNVD-2023-38194）、Schneider Electric IGSS Data Server 访问控制错误漏洞（CNVD-2023-38195）。除“Schneider Electric StruxureWare Data Center Expert 操作系统命令注入漏洞”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-2023-37595
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37594
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37593
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37592
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37598
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37597
https://www.cnvd.org.cn/flaw/show/CNVD-2023-38194
https://www.cnvd.org.cn/flaw/show/CNVD-2023-38195

### 3、 Adobe 产品安全漏洞

Adobe Substance 3D Stager 是美国奥多比（Adobe）公司的一个虚拟 3D 工作室。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超出已分配内存结构的末尾，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 Substance 3D Stager 越界读取漏洞（CNVD-2023-37604、CNVD-2023-37603、CNVD-2023-37606、CNVD-2023-37605、CNVD-2023-37608、CNVD-2023-37607）、Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2023-37602、CNVD-2023-37601）。除“Adobe Substance 3D Stager 越界读取漏洞（CNVD-2023-37608、CNVD-2023-37603）”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-2023-37604
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37603
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37602
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37601
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37606
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37605
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37608
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37607

### 4、IBM 产品安全漏洞

IBM Maximo Asset Management 是美国国际商业机器（IBM）公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。IBM Business Automation Workflow 是一个集成平台，可帮助业务用户大规模地快速自动完成业务运营的各个方面。IBM UrbanCode Deploy（UCD）是一套应用自动化部署工具。该工具基于一个应用部署自动化管理信息模型，并通过远程代理技术，实现对复杂应用在不同环境下的自动化部署等。IBM WebSphere Application Server（WAS）是一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。IBM Financial Transaction Manager for SWIFT Services 是一款金融事务管理器产品。该产品主要用于监控、跟踪和报告金融支付和交易。IBM Safer Payments 是美国 IBM 公司的第一个真正的支付处理认知欺诈预防解决方案。帮助客户创建定制的、用户友好的决策模型。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感密码信息，注入恶意的 JavaScript 脚本等。

CNVD 收录的相关漏洞包括：IBM Maximo Asset Management 跨站脚本漏洞（CNVD-2023-37159）、IBM Business Automation Workflow 跨站脚本漏洞（CNVD-2023-37162）、IBM UrbanCode Deploy 信息泄露漏洞（CNVD-2023-37161）、IBM WebSphe

re Application Server 信任管理问题漏洞、IBM Financial Transaction Manager for SWIFT Services 跨站脚本漏洞（CNVD-2023-37163）、IBM Safer Payments 加密问题漏洞、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2023-37168）、IBM Maximo Asset Management 信息泄露漏洞（CNVD-2023-37167）。其中，“IBM Safer Payments 加密问题漏洞”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-2023-37159
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37162
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37161
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37164
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37163
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37165
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37168
https://www.cnvd.org.cn/flaw/show/CNVD-2023-37167

**5、D-Link DIR-605L 堆栈缓冲区溢出漏洞**

D-Link DIR-605L 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-605L 被披露存在堆栈缓冲区溢出漏洞。攻击者可利用该漏洞使缓冲区溢出并在系统上执行任意代码，或者导致拒绝服务。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-2023-39044

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-2023-38197 | mySCADA myPRO 操作系统命令注入漏洞（CNVD-2023-38197） | 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-2023-39428 | phpMyFAQ 跨站脚本漏洞（CNVD-2023-39428） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/thorsten/phpmyfaq/commit/e7599d49b0ece7ceef3a4e8d334782cc3df98be8 |
| CNVD-2023-37156 | Huawei HiLink AI Life 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://www.huawei.com/en/psirt/security-advisories/2023/huawei-sa-ipav |

| | | | |
|---|---|---|---|
| | | | ihwhis-1556afc2-en |
| CNVD-2023-37594 | Schneider Electric StruxureWare Data Center Expert 访问控制错误漏洞（CNVD-2023-37594） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf |
| CNVD-2023-37592 | Schneider Electric StruxureWare Data Center Expert 访问控制错误漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-02.pdf |
| CNVD-2023-37602 | Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2023-37602） | 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/substance3d_stager/apsb23-26.html |
| CNVD-2023-37607 | Adobe Substance 3D Stager 越界读取漏洞（CNVD-2023-37607） | 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/substance3d_stager/apsb23-26.html |
| CNVD-2023-38962 | Huawei EMUI 和 HarmonyOS 信息泄露漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/en/support/bulletin/2023/1/ |
| CNVD-2023-38964 | Huawei EMUI 和 HarmonyOS 双重释放漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/en/support/bulletin/2023/1/ |
| CNVD-2023-39042 | ZTE MF297D 信息泄露漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1024624 |

小结：本周，Huawei 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信息，导致恶意隐藏应用程序图标，造成拒绝服务等。此外，Schneider Electric、Adobe、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞发送特制的消息来获取操作和读取 IGSS 项目报告目录中的文件，注入恶意的 JavaScript 脚本，在当前用户的上下文中执行任意代码等。另外，D-Link DIR-605L 被披露存在堆栈缓冲区溢出漏洞。攻击者

可利用该漏洞使缓冲区溢出并在系统上执行任意代码，或者导致拒绝服务。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、SIYUCMS 远程代码执行漏洞

**验证描述**

SIYUCMS 是一款基于 ThinkPHP+AdminLTE 的内容管理系统。

SIYUCMS 存在远程代码执行漏洞，攻击者可利用该漏洞获取服务器权限。

**验证信息**

POC 链接：https://github.com/cai-niao98/siyu

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-39103

**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. 三星设备受到攻击，新的安全漏洞被曝光

美国网络安全和基础设施安全局警告说，一个影响三星设备的漏洞正在被滥用，该漏洞被追踪为 CVE-2023-21492。

参考链接：https://www.freebuf.com/news/367168.html

### 2. 苹果公司“又又又”曝出漏洞

苹果表示公司内部已经知道了三个零日漏洞正在野外被积极利用，5 月 1 日发布的 iOS 16.4.1 和 macOS 13.3.1 设备的快速安全响应（RSR）补丁解决 CVE-2023-28204 和 CVE-2023-32373 这两个漏洞问题。

参考链接：https://www.bleepingcomputer.com/news/apple/apple-fixes-three-new-zero-days-exploited-to-hack-iphones-macs/

**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