# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2023 年 07 月 17 日-2023 年 07 月 23 日** **2023 年第 29 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 422 个，其中高危漏洞 258 个、中危漏洞 137 个、低危漏洞 27 个。漏洞平均分值为 6.85。本周收录的漏洞中，涉及 0day 漏洞 368 个（占 87%），其中互联网上出现“Online Piggery Management System 任意文件上传漏洞、EyouCms 跨站脚本漏洞（CNVD-2023-58096）”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 8721 个，与上周（11081 个）环比减少 21%。

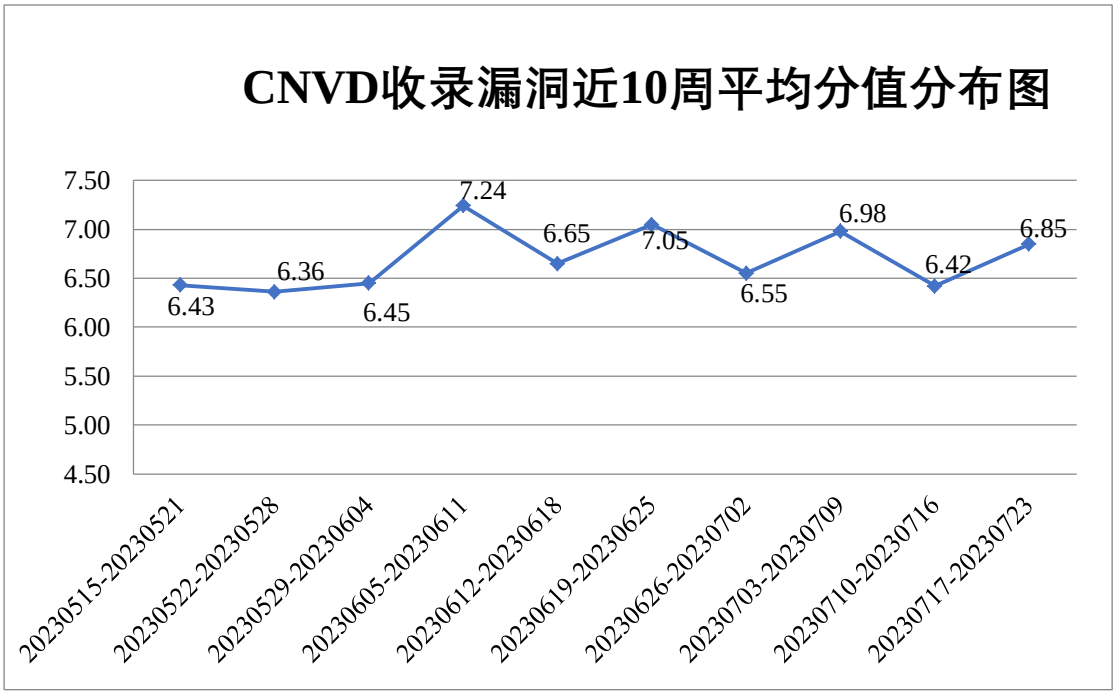


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 16 起，向基础电

信企业通报漏洞事件 14 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 1525 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 250 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 59 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：

卓豪（中国）技术有限公司、珠海格力电器股份有限公司、重庆猫扑网络科技有限公司、中建商品混凝土有限公司、中电鸿信信息科技有限公司、浙江小遛信息科技有限公司、浙江施强医疗科技有限公司、浙江环鑫信息技术有限公司、浙江和达科技股份有限公司、长沙正宇软件开发有限公司、长沙宏地科技开发有限公司、云南链滴科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永辉超市股份有限公司、银川中房物业集团股份有限公司、研华科技（中国）有限公司、兄弟（中国）商业有限公司、西安思铂电子科技有限公司、温州市万旗信息科技有限公司、威博通科技（上海）有限公司、网易公司、统信软件技术有限公司、同程网络科技股份有限公司、天津天堰科技股份有限公司、腾讯安全应急响应中心、泰安云豹网络科技有限公司、台达电子企业管理(上海)有限公司、苏州宏云智能科技有限公司、松下电器（中国）有限公司、四川迅睿云软件开发有限公司、四川蜀信致远企业管理咨询有限公司、施耐德电气（中国）有限公司、深圳致软信息技术有限公司、深圳维盟科技股份有限公司、深圳市亚略特科技股份有限公司、深圳市科脉技术股份有限公司、深圳市吉祥腾达科技有限公司、深圳市道尔智控科技股份有限公司、深圳典阅科技有限公司、上海纵之格科技有限公司、上海正广和饮用水有限公司、上海盈翼文化传播有限公司、上海淘满家电子商务有限公司、上海瑞策软件有限公司、上海华测导航技术股份有限公司、上海富勒信息科技有限公司、上海孚盟软件有限公司、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、山东云时空信息科技有限公司、山东博硕自动化技术有限公司、厦门市灵鹿谷科技有限公司、厦门计讯物联科技有限公司、三菱电机株式会社、青岛卓尔软件开发有限公司、南京博纳睿通软件科技有限公司、梅州市青云客网络科技有限公司、轮汇（辽宁）网络科技有限公司、联想集团、九江天一科技有限公司、京瓷办公信息系统（中国）有限公司、金华迪加网络科技有限公司、脚印兄弟(北京)信息科技有限责任公司、江西铭软科技有限公司、江苏银河电子股份有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、慧学教育科技(北京)有限公司、华硕电脑（上海）有限公司、湖南阿必达物流配送有限公司、红门智能科技股份有限公司、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、杭州炳炳其章网络科技有限公司、海恩斯莫里斯（上海）商业有限公司、桂林崇胜网络科技有限公司、贵阳语玩科技有限公司、广州安网通信技术有限公司、广东鑫宝软件科技有限公司、广东美胸汇网络科技有限公司、馥鸿科技股份有限公司、点都互联科技有限公司、大成方略纳税人俱乐部股份有限公司、

成都友加畅捷科技有限公司、成都延华西部健康医疗信息产业研究院有限公司、北京中文万维科技有限公司、北京中科华博科技有限公司、北京中海义信信息技术有限公司、北京云中融信网络科技有限公司、北京星网锐捷网络技术有限公司、北京小熊博望科技有限公司、北京通达信科科技有限公司、北京数字政通科技股份有限公司、北京书生云科技有限公司、北京世纪超星信息技术发展有限责任公司、北京金和网络股份有限公司、北京华夏春松科技有限公司、北京华品博睿网络技术有限公司、北京瀚维特科技有限公司、北京读书人网络科技有限公司、北京道亨软件股份有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、保联电脑股份有限公司、安美科技股份有限公司、爱普生（中国）有限公司、阿帕数字技术有限公司、nginxWEBUI 和 MuYuCMS。

本周，CNVD 发布了《Oracle 发布 2023 年 7 月的安全公告》和《Microsoft 发布 2023 年 7 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9046

https://www.cnvd.org.cn/webinfo/show/9041

## 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、深信服科技股份有限公司、安天科技集团股份有限公司、北京天融信网络安全技术有限公司、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。内蒙古中叶信息技术有限责任公司、重庆电信系统集成有限公司、杭州美创科技有限公司、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、联想集团、快页信息技术有限公司、河北锐远网络科技有限公司、赛尔网络有限公司、安徽锋刃信息科技有限公司、信息产业信息安全测评中心、智网安云（武汉）信息技术有限公司、河南信安世纪科技有限公司、杭州默安科技有限公司、北京微步在线科技有限公司、北京山石网科信息技术有限公司、河南省鼎信信息安全等级测评有限公司、山东九域信息技术有限公司、成都天天网安信息安全技术有限公司、南方电网数字电网集团信息通信科技有限公司、平安银河实验室、宁夏凯信特信息科技有限公司、南京深安科技有限公司、亚信科技（成都）有限公司、博智安全科技股份有限公司、浙江中控技术股份有限公司、北京惠而特科技有限公司、重庆易阅科技有限公司、中国电信股份有限公司研究院、西藏熙安信息技术有限责任公司及其他个人白帽子向 CNVD 提交了 8721 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）、上海交大、奇安信网神（补天平台）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 6818 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） | 3025 | 3025 |

| | | |
|---|---|---|
| 奇安信网神（补天平台） | 2384 | 2384 |
| 三六零数字安全科技集团有限公司 | 753 | 753 |
| 上海交大 | 656 | 656 |
| 新华三技术有限公司 | 419 | 0 |
| 深信服科技股份有限公司 | 347 | 0 |
| 安天科技集团股份有限公司 | 302 | 0 |
| 北京天融信网络安全技术有限公司 | 155 | 4 |
| 北京数字观星科技有限公司 | 150 | 0 |
| 阿里云计算有限公司 | 148 | 0 |
| 北京长亭科技有限公司 | 85 | 2 |
| 天津市国瑞数码安全系统股份有限公司 | 59 | 0 |
| 北京知道创宇信息技术有限公司 | 41 | 0 |
| 杭州迪普科技股份有限公司 | 19 | 0 |
| 南京众智维信息科技有限公司 | 14 | 14 |
| 卫士通信息产业股份有限公司 | 8 | 8 |
| 京东科技信息技术有限公司 | 6 | 6 |
| 北京神州绿盟科技有限公司 | 4 | 4 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 4 | 4 |
| 西安四叶草信息技术 | 3 | 3 |

| | | |
|---|---|---|
| 有限公司 | | |
| 华为技术有限公司 | 3 | 3 |
| 北京智游网安科技有限公司 | 2 | 2 |
| 南京铱迅信息技术股份有限公司 | 1 | 1 |
| 内蒙古中叶信息技术有限责任公司 | 93 | 93 |
| 重庆电信系统集成有限公司 | 80 | 80 |
| 杭州美创科技有限公司 | 72 | 72 |
| 奇安星城网络安全运营服务（长沙）有限公司 | 57 | 57 |
| 河南东方云盾信息技术有限公司 | 28 | 28 |
| 联想集团 | 18 | 18 |
| 快页信息技术有限公司 | 11 | 11 |
| 河北锎远网络科技有限公司 | 10 | 10 |
| 赛尔网络有限公司 | 8 | 8 |
| 安徽锋刃信息科技有限公司 | 7 | 7 |
| 信息产业信息安全测评中心 | 7 | 7 |
| 智网安云（武汉）信息技术有限公司 | 5 | 5 |
| 河南信安世纪科技有限公司 | 5 | 5 |
| 杭州默安科技有限公司 | 4 | 4 |
| 北京微步在线科技有限公司 | 4 | 4 |

| | | |
|---|---|---|
| 北京山石网科信息技术有限公司 | 4 | 4 |
| 河南省鼎信信息安全等级测评有限公司 | 3 | 3 |
| 山东九域信息技术有限公司 | 3 | 3 |
| 成都天天网安信息安全技术有限公司 | 3 | 3 |
| 南方电网数字电网集团信息通信科技有限公司 | 3 | 3 |
| 平安银河实验室 | 2 | 2 |
| 宁夏凯信特信息科技有限公司 | 2 | 2 |
| 南京深安科技有限公司 | 2 | 2 |
| 亚信科技（成都）有限公司 | 1 | 1 |
| 博智安全科技股份有限公司 | 1 | 1 |
| 浙江中控技术股份有限公司 | 1 | 1 |
| 北京惠而特科技有限公司 | 1 | 1 |
| 重庆易阅科技有限公司 | 1 | 1 |
| 中国电信股份有限公司研究院 | 1 | 1 |
| 西藏熙安信息技术有限责任公司 | 1 | 1 |
| 个人 | 1414 | 1414 |
| 报送总计 | 10440 | 8721 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 422 个漏洞。WEB 应用 289 个，网络设备（交换机、路由器等网络端设备）53 个，应用程序 50 个，操作系统 15 个，智能设备（物联网终端设备）14 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 | 289 |
| 网络设备（交换机、路由器等网络端设备） | 53 |
| 应用程序 | 50 |
| 操作系统 | 15 |
| 智能设备（物联网终端设备） | 14 |
| 安全产品 | 1 |

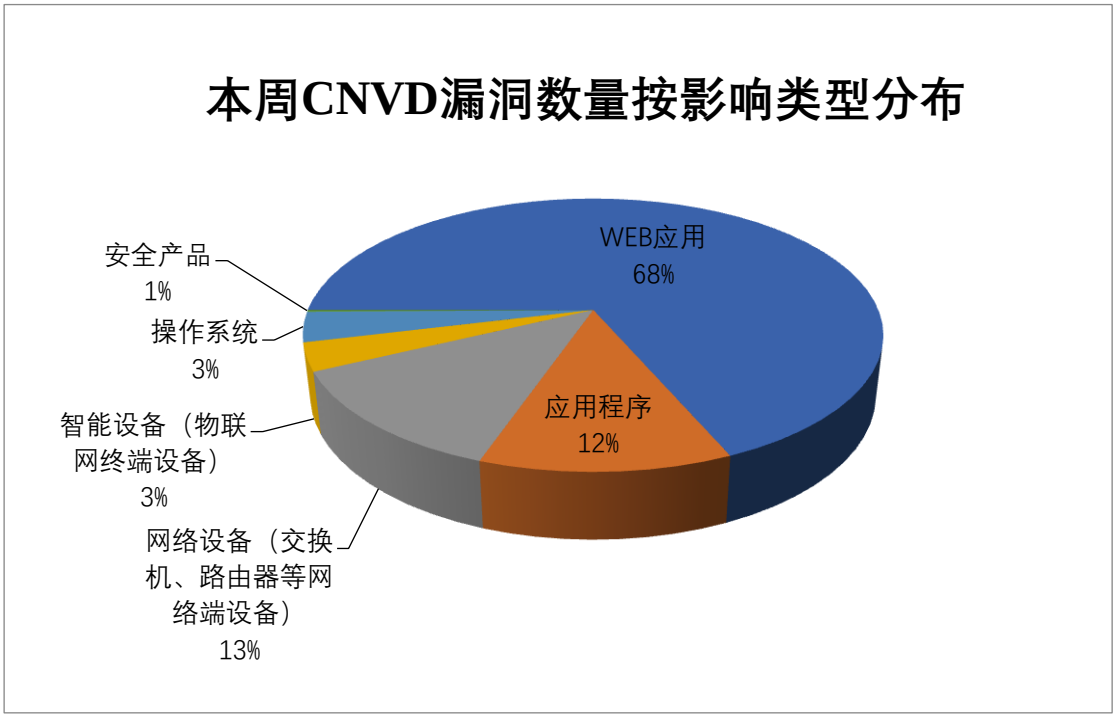


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Linux、Trend Micro 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 | D-Link | 20 | 5% |
| 2 | Linux | 12 | 3% |
| 3 | Trend Micro | 11 | 3% |
| 4 | Siemens | 10 | 2% |
| 5 | 深圳市必联电子有限公司 | 9 | 2% |

| | | | |
|---|---|---|---|
| 6 | 用友网络科技股份有限公司 | 9 | 2% |
| 7 | Adobe | 8 | 2% |
| 8 | 江西铭软科技有限公司 | 7 | 2% |
| 9 | 北京百卓网络技术有限公司 | 6 | 1% |
| 10 | 其他 | 330 | 78% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 28 个电信行业漏洞，21 个移动互联网行业漏洞，15 个工控行业漏洞（如下图所示）。其中，“H3C Magic R300 堆栈溢出漏洞（CNVD-2023-57673）、Siemens SIMATIC MV500 Devices 资源消耗失控漏洞”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/

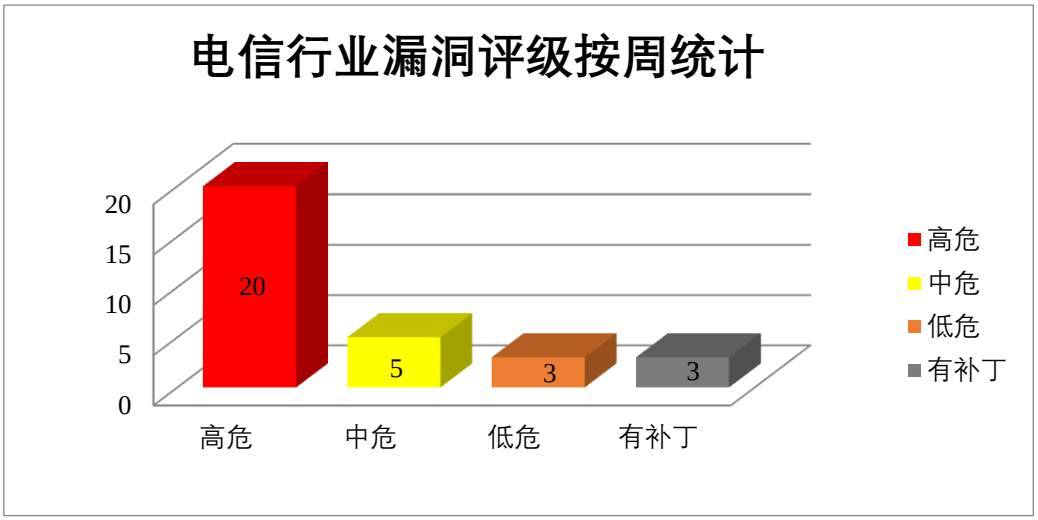


图 3 电信行业漏洞统计

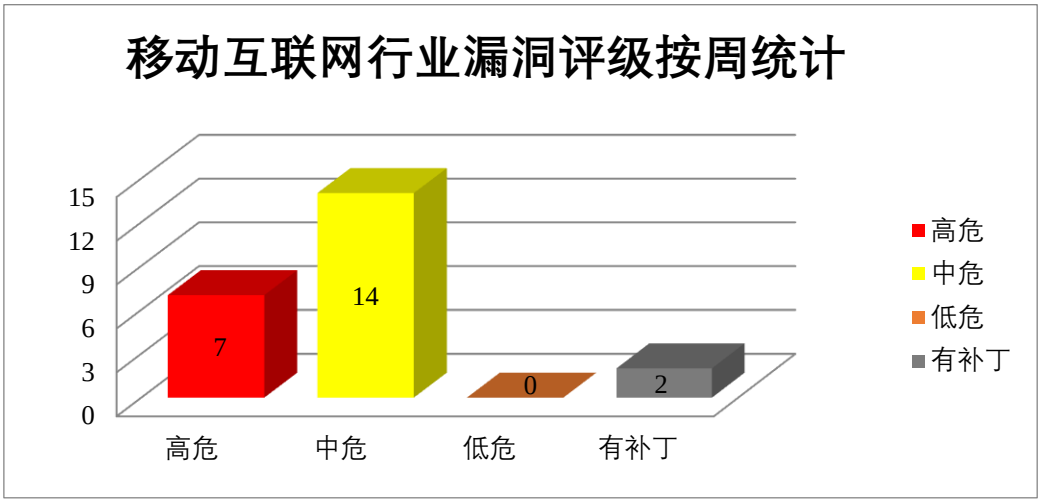


图 4 移动互联网行业漏洞统计

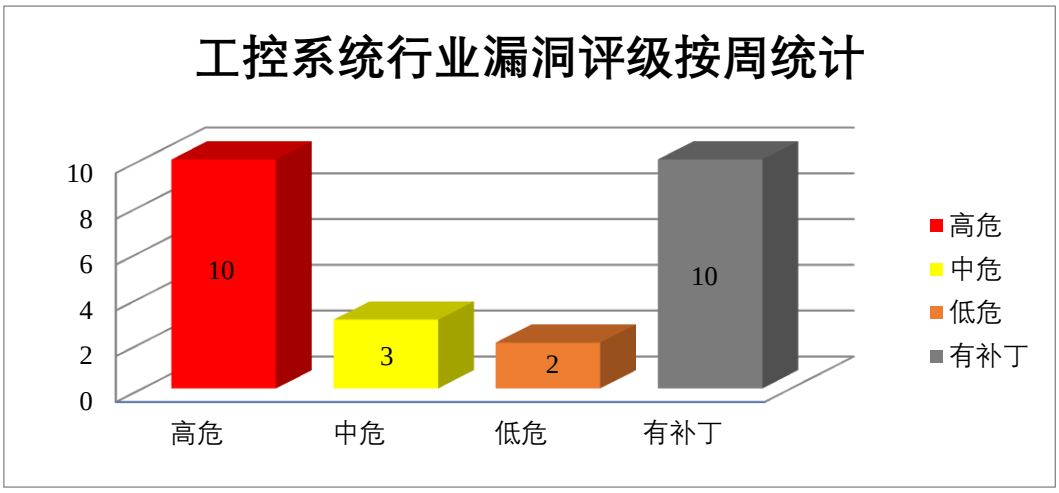


图 5 工控系统行业漏洞统计

## 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 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。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，导致敏感内存泄露等。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 访问控制错误漏洞（CNVD-2023-57681、CNVD-2023-57682）、Adobe Acrobat Reader 越界读取漏洞（CNVD-2023-57683、CNVD-2023-57685）、Adobe Acrobat Reader 越界写入漏洞（CNVD-2023-57687、CNVD-2023-57684、CNVD-2023-57688）、Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2023-57686）。其中，除“Adobe Acrobat Reader 越界读取漏洞（CNVD-2023-57685）”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-2023-57681
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57683
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57682
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57687
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57686
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57685
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57684
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57688

### 2、Trend Micro 产品安全漏洞

Trend Micro Apex Central 是美国趋势科技（Trend Micro）公司的一个基于 Web 的控制台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的 SQL 请求，操作数据库，获取敏感信息或执行任意代码，注入恶意脚本或 HTML 代码等。

CNVD 收录的相关漏洞包括：Trend Micro Apex Central 跨站脚本漏洞（CNVD-2023-57660、CNVD-2023-57666、CNVD-2023-57664、CNVD-2023-57663、CNVD-2023-57662、CNVD-2023-57661）、Trend Micro Apex Central SQL 注入漏洞（CNVD-2023-57667、CNVD-2023-57659）。其中，“Trend Micro Apex Central SQL 注入漏洞（CNVD-2023-57667、CNVD-2023-57659）”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-2023-57660
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57659
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57664
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57663
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57662
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57661
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57667
https://www.cnvd.org.cn/flaw/show/CNVD-2023-57666

### 3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，可使系统崩溃，造成拒绝服务攻击，导致在内核内存中执行任意读写等。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2023-56639、CNVD-2023-56644、CNVD-2023-56638）、Linux kernel 缓冲区溢出漏洞（CNVD-2023-56643、CNVD-2023-56648、CNVD-2023-56641）、Linux kernel cedrus.c 资源管理错误漏洞、Linux kernel 资源管理错误漏洞（CNVD-2023-56642）。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-2023-56638

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56641

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56639

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56644

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56643

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56642

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56648

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56647

### 4、Siemens 产品安全漏洞

Siemens SiPass Integrated 是德国西门子（Siemens）公司的一套门禁系统。Siemens Tecnomatix Plant Simulation 是德国西门子（Siemens）公司的工控设备，利用离散事件仿真进行生产量分析和优化，进而改善制造系统性能。SIMATIC MV500 产品是固定式光学读卡器，用于捕获各种不同表面上的打印、激光、钻孔、冲孔和点划线代码。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进程的上下文中执行代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens Tecnomatix Plant Simulation 堆栈缓冲区溢出漏洞（CNVD-2023-56535、CNVD-2023-56536）、Siemens Tecnomatix Plant Simulation 类型混淆漏洞、Siemens SiPass Integrated 堆栈溢出漏洞、Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-56537）、Siemens SIMATIC MV500 Devices 资源消耗失控漏洞（CNVD-2023-56540）、Siemens Tecnomatix Plant Simulation 堆缓冲区溢出漏洞（CNVD-2023-56539、CNVD-2023-56538）。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-2023-56535

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56534

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56533

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56537

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56536

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56540

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56539

https://www.cnvd.org.cn/flaw/show/CNVD-2023-56538

### 5、Tenda AC5 R7WebsSecurityHandler 函数缓冲区溢出漏洞

Tenda AC5 是中国腾达（Tenda）公司的一款无线路由器。本周，Tenda AC5 被披

露存在缓冲区溢出漏洞。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。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-2023-57680

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-2023-56538 | Siemens Tecnomatix Plant Simulation 堆缓冲区溢出漏洞（CNVD-2023-56538） | 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://cert-portal.siemens.com/productcert/html/ssa-764801.html |
| CNVD-2023-56541 | Siemens SIMATIC MV500 Devices 资源消耗失控漏洞（CNVD-2023-56541） | 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://cert-portal.siemens.com/productcert/html/ssa-561322.html |
| CNVD-2023-57670 | Apache Portable Runtime 越界写漏洞（CNVD-2023-57670） | 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/5pfdfn7h0vsdo5xzjn97vghp0x42jj2r |
| CNVD-2023-57672 | Apache Portable Runtime 越界写漏洞 | 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/fw9p6sdncwsjkstwc066vz57xqzfksq9 |
| CNVD-2023-57674 | H3C Magic R300 堆栈溢出漏洞（CNVD-2023-57674） | 高 | 用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.h3c.com/ |
| CNVD-2023-57675 | H3C Magic R300 堆栈溢出漏洞（CNVD-2023-57675） | 高 | 用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.h3c.com/ |
| CNVD-2023-57676 | Huawei HarmonyOS 和 EMUI 存储模块身份验证错误漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202307-0000001587168858 |
| CNVD-2023-57677 | Huawei HarmonyOS 和 EMUI AMS 模块安全绕过漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202307-0000001587168858 |
| CNVD-2023-57687 | Adobe Acrobat Reader 越界写入漏洞 | 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/acrobat/apsb23-01.html |
| CNVD-2023-57688 | Adobe Acrobat Reader 越界写入漏洞（CNVD-2023-57688） | 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/acrobat/apsb23-01.html |

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，导致敏感内存泄露等。此外，Trend Micro、Linux、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的 SQL 请求，操作数据库，获取敏感信息或执行任意代码，注入恶意脚本或 HTML 代码，造成拒绝服务攻击，导致在内核内存中执行任意读写等。另外，Tenda AC5 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞使缓冲区溢出并在系统上执行任意代码。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、EyouCms 跨站脚本漏洞（CNVD-2023-58096）

**验证描述**

EyouCms 是一套基于 ThinkPHP 的开源内容管理系统（CMS）。

EyouCms 存在跨站脚本漏洞，该漏洞源于 Column management 模块对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过精心制作的有效负载执行任意 web 脚本或 HTML。

**验证信息**

POC 链接：https://github.com/weng-xianhu/eyoucms/issues/46

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-58096

**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. Apache OpenMeetings 网络会议工具曝出安全漏洞

网络会议服务 Apache OpenMeetings 存在多个安全漏洞，Sonar 漏洞研究员 Stefan Schiller 表示网络攻击者可以利用这些漏洞夺取管理帐户的控制权，并在易受影响的服

务器上执行恶意代码。

参考链接：https://thehackernews.com/2023/07/apache-openmeetings-web-conferencing.html

### 2. 云计算供应链遭遇安全风险，AMI MegaRAC BMC 曝两大安全漏洞

近日，AMI MegaRAC Baseboard Management Controller (BMC)软件中披露了两个安全漏洞，这些漏洞一旦被攻击者成功利用，将可远程控制服务器并直接部署恶意软件。

参考链接：https://thehackernews.com/2023/07/critical-flaws-in-ami-megarac-bmc.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