# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2024 年 07 月 08 日-2024 年 07 月 14 日** **2024 年第 28 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 329 个，其中高危漏洞 155 个、中危漏洞 158 个、低危漏洞 16 个。漏洞平均分值为 6.52。本周收录的漏洞中，涉及 0day 漏洞 216 个（占 66%），其中互联网上出现“Tenda AC10U 堆栈缓冲区溢出漏洞（CNVD-2024-31493、CNVD-2024-31494）”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 19961 个，与上周（17463 个）环比增加 14%。

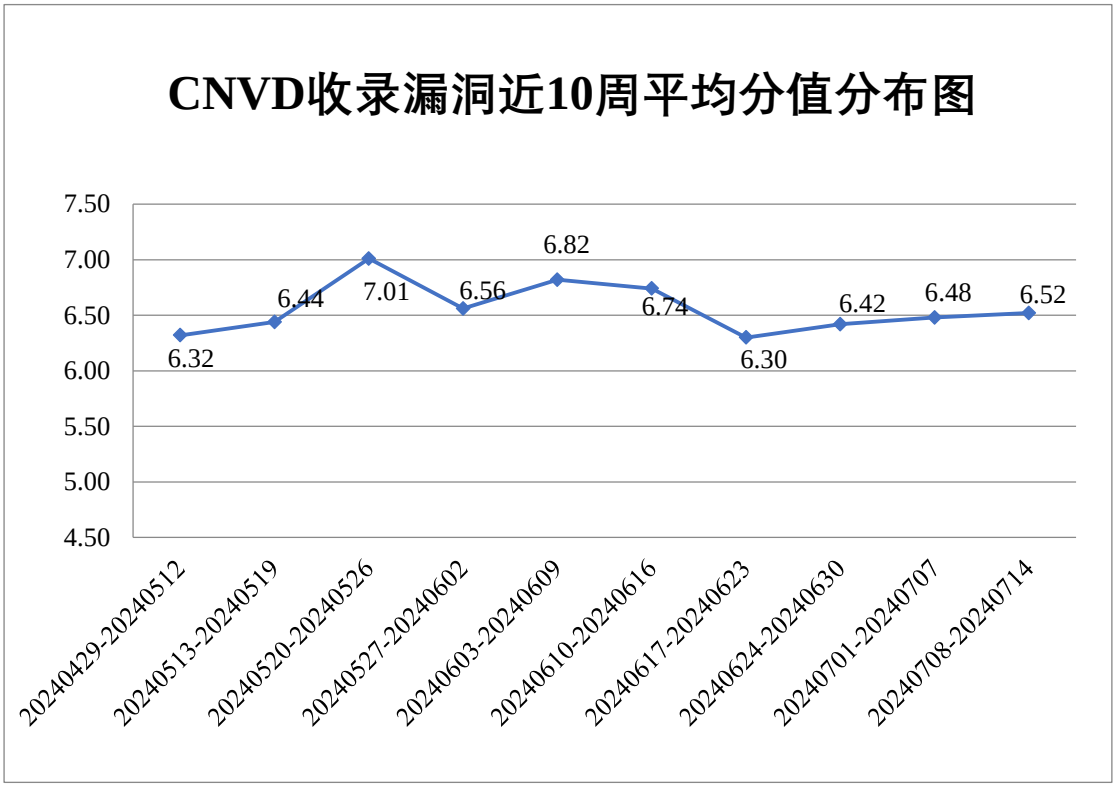


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 11 起，向基础电信企业通报漏洞事件 8 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 951 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 132 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 14 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：

紫光软件系统有限公司、珠海派诺科技股份有限公司、珠海奔图电子有限公司、中科商软软件有限公司、中科博华信息科技有限公司、正元智慧集团股份有限公司、正方软件股份有限公司、浙江码尚科技股份有限公司、浙江和达科技股份有限公司、浙江好络维医疗技术有限公司、浙江大华技术股份有限公司、远盟康健科技有限公司、用友网络科技股份有限公司、阳光电源股份有限公司、新都（青岛）办公设备有限公司、新道科技股份有限公司、西安新途数字科技有限公司、西安瑞友信息技术资讯有限公司、武汉中地数码科技有限公司、武汉天地伟业科技有限公司、武汉明源动力软件有限公司、温州市易天信息科技有限公司、卫宁健康科技集团股份有限公司、微软（中国）有限公司、统信软件技术有限公司、腾讯安全应急响应中心、唐山市柳林自动化设备有限公司、泰安梦泰尔软件有限公司、索尼（中国）有限公司、随锐科技集团股份有限公司、苏州科达科技股份有限公司、沈阳盘古网络技术有限公司、深圳市亚略特科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市宏电技术股份有限公司、深圳市博思协创网络科技有限公司、深圳市必联电子有限公司、深圳开维信息技术股份有限公司、深圳古瑞瓦特科技能源有限责任公司、申瓯通信设备有限公司、上海装盟信息科技有限公司、上海熠知电子科技有限公司、上海商汤智能科技有限公司、上海桑锐电子科技股份有限公司、上海三高计算机中心股份有限公司、上海宁盾信息科技有限公司、上海肯特仪表股份有限公司、上海布雷德科技有限公司、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、厦门科拓通讯技术股份有限公司、厦门凤凰创壹软件有限公司、三星（中国）投资有限公司、三未信安科技股份有限公司、若依、融智通科技（北京）股份有限公司、青岛海尔生物医疗股份有限公司、麒麟软件有限公司、普元信息技术股份有限公司、普信恒业科技发展（北京）有限公司、南宁迈世信息技术有限公司、南京云网汇联软件技术有限公司、南京先维信息技术有限公司、南京酷奇信息科技有限公司、南昌航天广信科技有限责任公司、迈普通信技术股份有限公司、利盟信息技术（中国）有限公司、京瓷（中国）商贸有限公司、江苏赛达电子科技有限公司、江苏麦维智能科技有限公司、佳能（中国）有限公司、济南优力电子科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖北双可科技有限公司、河北先河环保科技股份有限公司、杭州伊柯夫科技有限公司、杭州雄伟科技开发股份有

限公司、杭州雄迈信息技术有限公司、杭州新中大科技股份有限公司、杭州阔知网络科技有限公司、杭州海康威视数字技术股份有限公司、杭州贝腾科技有限公司、海口快推科技有限公司、国子软件股份有限公司、广州市巨控电子科技有限公司、广联达科技股份有限公司、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、富士施乐（中国）有限公司、福建星网锐捷通讯股份有限公司、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、大庆紫金桥软件技术有限公司、成都德芯数字科技股份有限公司、超聚变数字技术有限公司、畅捷通信息技术股份有限公司、北京佐卡科技有限公司、北京中创视讯科技有限公司、北京智慧云巅科技有限公司、北京致远互联软件股份有限公司、北京亿信华宇软件有限责任公司、北京亿赛通科技发展有限责任公司、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、北京网御星云信息技术有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京人大金仓信息技术股份有限公司、北京美特软件技术有限公司、北京朗新天霁软件技术有限公司、北京金和网络股份有限公司、北京杰控科技有限公司、北京慧图科技（集团）股份有限公司、北京惠朗时代科技有限公司、北京百卓网络技术有限公司、北京百容千域软件技术开发有限责任公司、傲拓科技股份有限公司、安科瑞电气股份有限公司和爱普生（中国）有限公司。

本周，CNVD 发布了《Microsoft 发布 2024 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/10201）。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，安天科技集团股份有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司、天津市国瑞数码安全系统股份有限公司等单位报送公开收集的漏洞数量较多。成都卫士通信息安全技术有限公司、江苏金盾检测技术股份有限公司、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、北京翰慧投资咨询有限公司、北京中睿天下信息技术有限公司、成都久信信息技术股份有限公司、江苏云天网络安全技术有限公司、快页信息技术有限公司、厦门聚丁科技有限公司、福建中信网安信息科技有限公司、即现（信阳）网络科技有限公司、上海直画科技有限公司、重庆都会信息科技有限公司、比亚迪股份有限公司、江苏极元信息技术有限公司、上海亿保健康科技集团有限公司、上海谋乐网络科技有限公司、内蒙古洞明科技有限公司、江苏晟晖信息科技有限公司、中国电信股份有限公司上海研究院、河南灵创电子科技有限公司、河南宝通信息安全测评有限公司、成方金融科技有限公司上海分公司、深圳昂楷科技有限公司、安徽天行网安信息安全技术有限公司、江西中和证信息安全技术有限公司、南京聚铭网络科技有限公司、甘肃赛飞安全科技有限公司、亚信科技（成都）有限公司、中华人民共和国上海海事局、杭州默安科技

有限公司、四川奇安旌服科技有限公司、联通数字科技有限公司、北京远禾科技有限公司、马鞍山书拓安全科技有限公司、山石网科通信技术股份有限公司、中资网络信息安全科技有限公司、江苏百达智慧网络科技有限公司（含光实验室）、苏州棱镜七彩信息科技有限公司、西安市大数据服务中心、贵州蓝天创新科技有限公司、南京深安科技有限公司、上海观安信息技术股份有限公司、广州华南检验检测中心有限公司、杭州孝道科技有限公司、上海只柏特信息技术有限公司、湖南泛联新安信息科技有限公司、四川电科宏安科技有限公司、交通运输部南海航海保障中心、北京六方云信息技术有限公司、联想集团及其他个人白帽子向 CNVD 提交了 19961 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）、三六零数字安全科技集团有限公司、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 18122 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 | 原创漏洞数量 |
|---|---|---|
| 奇安信网神（补天平台） | 14706 | 14706 |
| 三六零数字安全科技集团有限公司 | 1811 | 1811 |
| 斗象科技（漏洞盒子） | 1223 | 1223 |
| 安天科技集团股份有限公司 | 695 | 0 |
| 新华三技术有限公司 | 635 | 0 |
| 北京神州绿盟科技有限公司 | 525 | 1 |
| 北京数字观星科技有限公司 | 411 | 0 |
| 上海交大 | 382 | 382 |
| 天津市国瑞数码安全系统股份有限公司 | 192 | 0 |
| 阿里云计算有限公司 | 172 | 0 |
| 杭州安恒信息技术股份有限公司 | 121 | 121 |
| 北京安信天行科技有限公司 | 90 | 90 |
| 北京长亭科技有限公司 | 67 | 2 |
| 北京启明星辰信息安 | 66 | 1 |

| | | |
|---|---|---|
| 全技术有限公司 | | |
| 恒安嘉新（北京）科技股份公司 | 51 | 0 |
| 北京知道创宇信息技术有限公司 | 45 | 0 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 20 | 20 |
| 南京众智维信息科技有限公司 | 11 | 11 |
| 长春嘉诚信息技术股份有限公司 | 4 | 4 |
| 北京天融信网络安全技术有限公司 | 4 | 4 |
| 中国电信股份有限公司网络安全产品运营中心 | 3 | 3 |
| 北京信联数安科技有限公司 | 2 | 2 |
| 成都卫士通信息安全技术有限公司 | 104 | 104 |
| 江苏金盾检测技术股份有限公司 | 50 | 50 |
| 西门子（中国）有限公司 | 33 | 0 |
| 河南东方云盾信息技术有限公司 | 29 | 29 |
| 北京山石网科信息技术有限公司 | 12 | 12 |
| 北京翰慧投资咨询有限公司 | 11 | 11 |
| 北京中睿天下信息技术有限公司 | 11 | 11 |
| 成都久信信息技术股份有限公司 | 11 | 11 |

| | | |
|---|---|---|
| 江苏云天网络安全技术有限公司 | 11 | 11 |
| 快页信息技术有限公司 | 11 | 11 |
| 厦门聚丁科技有限公司 | 7 | 7 |
| 福建中信网安信息科技有限公司 | 7 | 7 |
| 即现（信阳）网络科技有限公司 | 6 | 6 |
| 上海直画科技有限公司 | 6 | 6 |
| 重庆都会信息科技有限公司 | 4 | 4 |
| 比亚迪股份有限公司 | 3 | 3 |
| 江苏极元信息技术有限公司 | 3 | 3 |
| 上海亿保健康科技集团有限公司 | 3 | 3 |
| 上海谋乐网络科技有限公司 | 3 | 3 |
| 内蒙古洞明科技有限公司 | 3 | 3 |
| 江苏晟晖信息科技有限公司 | 3 | 3 |
| 中国电信股份有限公司上海研究院 | 2 | 2 |
| 河南灵创电子科技有限公司 | 2 | 2 |
| 河南宝通信息安全测评有限公司 | 2 | 2 |
| 成方金融科技有限公司上海分公司 | 2 | 2 |
| 深圳昂楷科技有限公司 | 2 | 2 |

| | | |
|---|---|---|
| 安徽天行网安信息安全技术有限公司 | 2 | 2 |
| 江西中和证信息安全技术有限公司 | 2 | 2 |
| 南京聚铭网络科技有限公司 | 2 | 2 |
| 甘肃赛飞安全科技有限公司 | 2 | 2 |
| 亚信科技（成都）有限公司 | 1 | 1 |
| 中华人民共和国上海海事局 | 1 | 1 |
| 杭州默安科技有限公司 | 1 | 1 |
| 四川奇安旌服科技有限公司 | 1 | 1 |
| 联通数字科技有限公司 | 1 | 1 |
| 北京远禾科技有限公司 | 1 | 1 |
| 马鞍山书拓安全科技有限公司 | 1 | 1 |
| 山石网科通信技术股份有限公司 | 1 | 1 |
| 中资网络信息安全科技有限公司 | 1 | 1 |
| 江苏百达智慧网络科技有限公司（含光实验室） | 1 | 1 |
| 苏州棱镜七彩信息科技有限公司 | 1 | 1 |
| 西安市大数据服务中心 | 1 | 1 |
| 贵州蓝天创新科技有限公司 | 1 | 1 |

| | | |
|---|---|---|
| 南京深安科技有限公司 | 1 | 1 |
| 上海观安信息技术股份有限公司 | 1 | 1 |
| 广州华南检验检测中心有限公司 | 1 | 1 |
| 杭州孝道科技有限公司 | 1 | 1 |
| 上海只柏特信息技术有限公司 | 1 | 1 |
| 湖南泛联新安信息科技有限公司 | 1 | 1 |
| 四川电科宏安科技有限公司 | 1 | 1 |
| 交通运输部南海航海保障中心 | 1 | 1 |
| 北京六方云信息技术有限公司 | 1 | 1 |
| 联想集团 | 2 | 2 |
| CNCERT 宁夏分中心 | 4 | 4 |
| CNCERT 河北分中心 | 1 | 1 |
| 个人 | 1235 | 1235 |
| 报送总计 | 22849 | 19961 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 329 个漏洞。按类型划分包括 WEB 应用 177 个，应用程序 46 个，网络设备（交换机、路由器等网络端设备）45 个，操作系统 32 个，智能设备（物联网终端设备）23 个，数据库 4 个，安全产品 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 | 177 |
| 应用程序 | 46 |
| 网络设备（交换机、路由器等网络端设备） | 45 |
| 操作系统 | 32 |
| 智能设备（物联网终端设备） | 23 |

| | |
|---|---|
| 数据库 | 4 |
| 安全产品 | 2 |

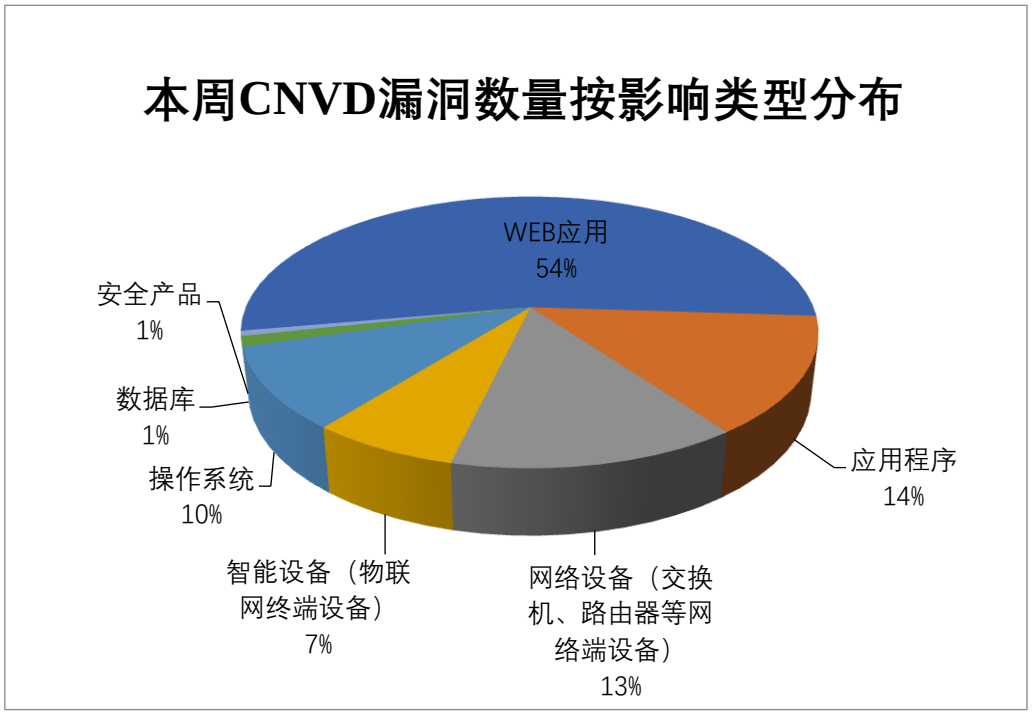


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、DELL、Huawei 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 | Siemens | 23 | 7% |
| 2 | DELL | 17 | 5% |
| 3 | Huawei | 17 | 5% |
| 4 | 北京神州视翰科技有限公司 | 12 | 4% |
| 5 | Adobe | 10 | 3% |
| 6 | Tenda | 9 | 3% |
| 7 | 北京金和网络股份有限公司 | 7 | 2% |
| 8 | 厦门科拓通讯技术股份有限公司 | 6 | 2% |
| 9 | 申瓯通信设备有限公司 | 6 | 2% |
| 10 | 其他 | 222 | 67% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 26 个电信行业漏洞，22 个移动互联网行业漏洞，18 个工控行业漏洞（如下图所示）。其中，“IBM WebSphere Application Server 代码执行漏洞（CNVD-2024-31485）、Rockwell Automation FactoryTalk View SE 身份验证错误漏洞、Huawei HarmonyOS 和 EMUI 拒绝服务漏洞（CNVD-2024-31528）”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/

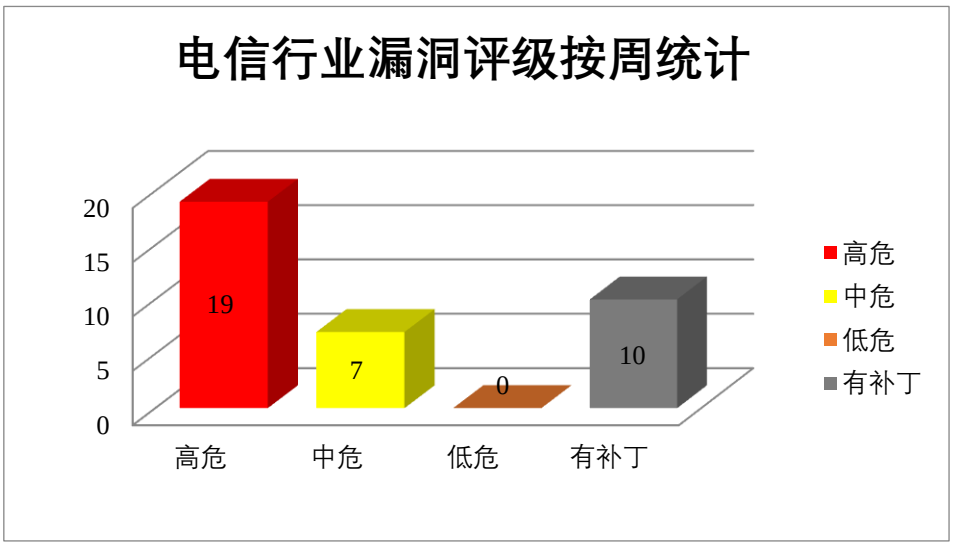


图 3 电信行业漏洞统计

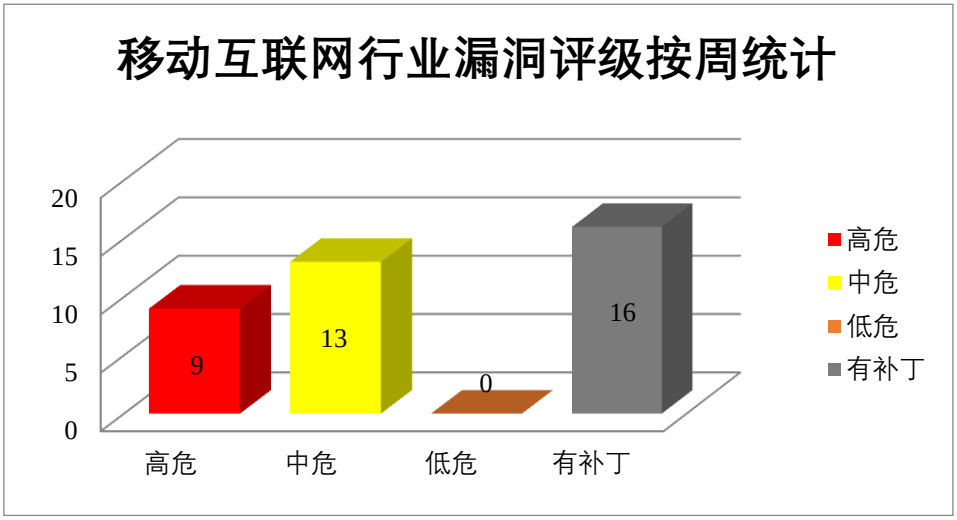


图 4 移动互联网行业漏洞统计

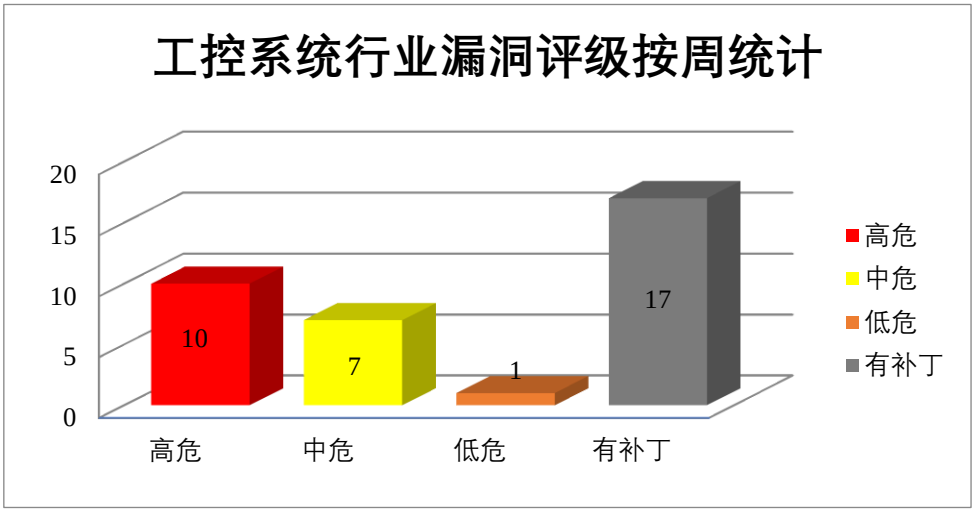


图 5 工控系统行业漏洞统计

## 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、 Siemens 产品安全漏洞

Siemens SINEMA Remote Connect Server 是德国西门子（Siemens）公司的一套远程网络管理平台。该平台主要用于远程访问、维护、控制和诊断底层网络。Siemens RuggedCom ROS 是德国西门子（Siemens）公司的一套用于 RuggedCom 系列交换机中的操作系统。Siemens Simcenter Femap 是德国西门子（Siemens）公司的一款尖端工程学仿真应用程序。用于创建、编辑和导入/重用复杂产品或系统基于网格的有限元分析模型。Siemens Teamcenter Visualization 是一个可为设计 2D、3D 场景提供团队协作功能的软件。Siemens JT2Go 是一款 JT 文件查看器。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，在当前进程的上下文中执行代码等。

CNVD 收录的相关漏洞包括：Siemens SINEMA Remote Connect Server 文件上传漏洞、Siemens SINEMA Remote Connect Server 使用不安全操作定义权限漏洞、Siemens RUGGEDCOM ROS 信息泄露漏洞（CNVD-2024-31234、CNVD-2024-31237）、Siemens Simcenter Femap 越界读取漏洞（CNVD-2024-31240、CNVD-2024-31239）、Siemens Simcenter Femap 越界写入漏洞（CNVD-2024-31241）、Siemens Teamcenter Visualization 和 JT2Go 越界读取漏洞（CNVD-2024-31244）。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-2024-31233

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31232

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31234

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31237

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31240

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31239

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31241

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31244

### 2、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，攻击者可利用漏洞查看系统上的任意文件，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：Huawei HarmonyOS 和 EMUI 拒绝服务漏洞（CNVD-2024-31073、CNVD-2024-31524、CNVD-2024-31525、CNVD-2024-31528）、Huawei HarmonyOS 和 EMUI 邮件模块脚本注入漏洞、Huawei HarmonyOS 和 EMUI 目录遍历漏洞、Huawei HarmonyOS 和 EMUI 安全绕过漏洞（CNVD-2024-31527）、Huawei HarmonyOS 和 EMUI 信息泄露漏洞（CNVD-2024-31529）。其中，除“Huawei HarmonyOS 和 EMUI 拒绝服务漏洞（CNVD-2024-31073）”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-2024-31073

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31083

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31524

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31525

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31526

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31527

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31528

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31529

### 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。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-31255、CNVD-2024-31254、CNVD-2024-31253、CNVD-2024-31252、CNVD-2024-31257、CNVD-2024-31256、CNVD-2024-31261、CNVD-2024-31260）。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-2024-31255

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31254

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31253

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31252

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31257

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31256

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31261

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31260

### 4、Dell 产品安全漏洞

Dell PowerProtect Data Domain 是美国戴尔（Dell）公司的一套用于数据保护、备份、存储和重复数据消除的硬件设备。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，注入恶意 HTML 或 JavaScript 代码等。

CNVD 收录的相关漏洞包括：Dell PowerProtect Data Domain 操作系统命令注入漏洞（CNVD-2024-31085）、Dell PowerProtect Data Domain 服务器端请求伪造漏洞、Dell PowerProtect Data Domain 跨站脚本漏洞、Dell PowerProtect Data Domain 开放重定向漏洞、Dell PowerProtect DM5500 目录遍历漏洞、Dell PowerProtect Data Domain 目录遍历漏洞、Dell PowerProtect Data Domain 日志信息泄露漏洞、Dell PowerProtect Data Domain 缓冲区溢出漏洞。其中，“Dell PowerProtect Data Domain 操作系统命令注入漏洞（CNVD-2024-31085）、Dell PowerProtect DM5500 目录遍历漏洞、Dell PowerProtect Data Domain 缓冲区溢出漏洞”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-2024-31085

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31088

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31087

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31086

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31093

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31092

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31091

https://www.cnvd.org.cn/flaw/show/CNVD-2024-31090

### 5、TOTOLINK EX1800T 命令执行漏洞（CNVD-2024-31498）

TOTOLINK EX1800T 是中国吉翁电子（TOTOLINK）公司的一款 Wi-Fi 范围扩展器。本周，TOTOLINK EX1800T 被披露存在命令执行漏洞。攻击者可利用该漏洞在系统上执行任意命令。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-2024-31498

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-2024-30839 | Rejetto HTTP File Server 模板注入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/rejetto/hfs/releases |
| CNVD-2024-30909 | Rockwell Automation FactoryTalk View SE 身份验证错误漏洞（CNVD-2024-30909） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1675.html |
| CNVD-2024-31394 | IBM Security Verify Access 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://www.ibm.com/support/pages/node/7158790 |
| CNVD-2024-31392 | Juniper Networks Junos OS 拒绝服务漏洞（CNVD-2024-31392） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://supportportal.juniper.net/JSA83195 |
| CNVD-2024-31398 | Foxit PDF Reader 远程代码执行漏洞（CNVD-2024-31398） | 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://www.foxit.com/support/security-bulletins.html |
| CNVD-2024-31487 | Mattermost 授权不当漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://mattermost.com/security-updates |
| CNVD-2024-31485 | IBM WebSphere Application Server 代码执行漏洞（CNVD-2024-31485） | 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/7159825 |
| CNVD-2024-31521 | Ffmpeg copy_column 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://trac.ffmpeg.org/ticket/10950 |
| CNVD-2024-30884 | Rockwell Automation FactoryTalk View SE 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://www.rockwellautomation.com/en-us/trust-center/security-advisories |

| | | | |
|---|---|---|---|
| | | | /advisory.SD1676.html |
| CNVD-2024-31518 | FFmpeg 缓冲区溢出漏洞（CNVD-2024-31518） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/FFmpeg/FFmpeg/commit/4565747056a11356210ed8edcecb920105e40b60 |

小结：本周，Siemens 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，在当前进程的上下文中执行代码等。此外，Huawei、Adobe、Dell 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 EX1800T 被披露存在命令执行漏洞。攻击者可利用该漏洞在系统上执行任意命令。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、Tenda AC10U 堆栈缓冲区溢出漏洞（CNVD-2024-31493）

**验证描述**

Tenda AC10U 是中国腾达（Tenda）公司的一款无线路由器。

Tenda AC10U 存在堆栈缓冲区溢出漏洞，该漏洞是由于 fromNatStaticSetting 函数的边界检查不正确造成的。攻击者可利用该漏洞在系统上执行任意代码。

**验证信息**

POC 链接：https://github.com/yaoyue123/iot/blob/main/Tenda/AC10U/fromNatStaticSetting.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-31493

**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. 官方强烈建议升级，GitLab 又曝账户接管漏洞

7 月 10 日，GitLab 警告称，其产品 GitLab 社区和企业版本中存在一个安全漏洞，允许攻击者以任何其他用户的身份运行管道作业。

参考链接：https://www.freebuf.com/news/405728.html

### 2. VMware Aria 自动化漏洞让黑客执行 SQL 注入攻击

VMware 发布了安全更新，以解决其 Aria Automation 产品中的 SQL 注入漏洞。跟踪为 CVE-2024-22280 的漏洞可能允许经过身份验证的攻击者执行未经授权的数据库操作。

参考链接：https://cybersecuritynews.com/vmware-aria-automation-sql-injection/

### 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