# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2021 年 11 月 08 日-2021 年 11 月 14 日　　2021 年第 45 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 484 个，其中高危漏洞 104 个、中危漏洞 328 个、低危漏洞 52 个。漏洞平均分值为 5.58。本周收录的漏洞中，涉及 0day 漏洞 344 个（占 71%），其中互联网上出现“webTareas 路径遍历漏洞、webTareas 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事件型漏洞总数 20493 个，与上周（13110 个）环比增加 56%。

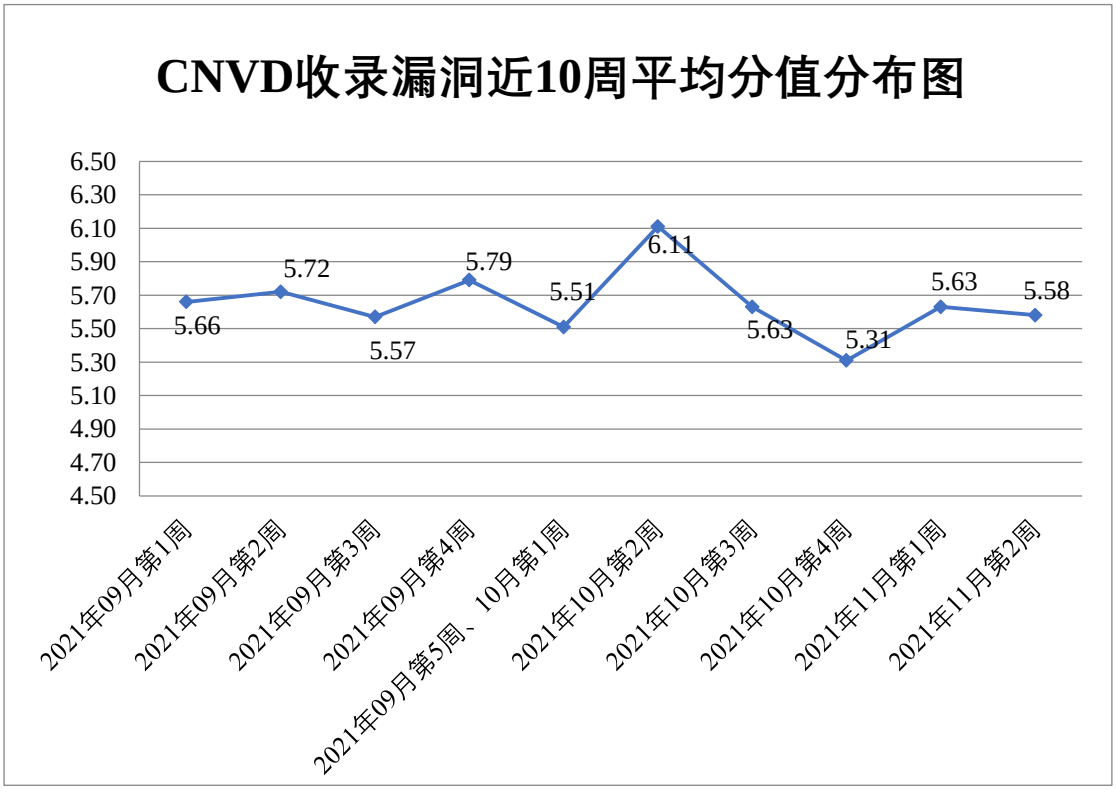


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 24 起，向基础电信企业通报漏洞事件 28 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 623 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 147 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 54 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：

淄博闪灵网络科技有限公司、珠海玖时光科技有限公司、重庆新光互动科技有限公司、重庆华人会信息技术有限公司、中新网络信息安全股份有限公司、中建西部建设股份有限公司、中国电信集团公司、浙江中易慧能科技有限公司、长沙友点软件科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、烟台晴好网络科技有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、新都（青岛）办公系统有限公司、西安九佳易信息资讯有限公司、武汉达梦数据库股份有限公司、微软（中国）有限公司、同望科技股份有限公司、通力电梯有限公司、宿迁鑫潮信息技术有限公司、松下电器（中国）有限公司、世邦通信股份有限公司、石家庄捷搜网络科技有限公司、深圳市友华通信技术有限公司、深圳市迅捷通信技术有限公司、深圳市西迪特科技有限公司、深圳市深日科技有限公司、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、深圳市朝恒辉网络科技有限公司、深圳极速创想科技有限公司、深圳华望技术有限公司、绍兴市青年软件开发有限公司、上海华测导航技术股份有限公司、上海创图网络科技股份有限公司、山东领图信息科技股份有限公司、厦门网中网软件有限公司、厦门凤凰创壹软件有限公司、全讯汇聚网络科技（北京）有限公司、普联技术有限公司、南京科远智慧科技集团股份有限公司、南京华设科技股份有限公司、摩莎科技（上海）有限公司、煤炭科学研究总院研究生院、龙采科技集团有限责任公司、廊坊市极致网络科技有限公司、昆明云涛科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、华为技术有限公司、合肥优视嵌入式技术有限责任公司、合肥久鑫网络科技有限公司、杭州顺网科技股份有限公司、汉王科技股份有限公司、桂林佳朋信息科技有限公司、贵州奥德网络科技有限公司、广州市成格信息技术有限公司、广州猎客软件科技有限公司、广东旭诚科技有限公司、富泰华工业（深圳）有限公司、福州网钛软件科技有限公司、福建银达汇智信息科技股份有限公司、福建星网锐捷通讯股份有限公司、帆软软件有限公司、东莞市信源计算机科技股份有限公司、得力集团有限公司、戴尔（中国）有限公司、大唐电信科技股份有限公司、大连龙采科技开发有限公司、成都万江港利科技股份有限公司、成都生动网络科技有限公司、成都爱诚科技有限公司、贝尔金国际有限公司、北京中远麒麟科技有限公司、北京中创视讯科技有限公司、北京中成科信科技发展有限公司、北京星网锐捷网络技术有限公司、北京伟业前程科技有限公司、北京网康科技有限公司、北京通达志成科技有限公司、北京通达信科科技有限公司、

北京上元信安技术有限公司、北京康心心理信息技术有限公司、北京火星高科数字科技有限公司、北京汉邦高科数字技术股份有限公司、北京碧海威科技有限公司、北京奥博威斯科技有限公司、奥壹科技(广州)有限公司、安科讯（福建）科技有限公司、无忧网络、若依、京瓷办公信息系统株式会社、zzcms、XnSoft、wazuh、Velos LLC、The Apache Software Foundation、Sapido Technology Inc、phpyun、Nacos、MuuCmf、Hancom、Genexis 和 Bandisoft。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京奇虎科技有限公司、新华三技术有限公司、哈尔滨安天科技集团股份有限公司、厦门服云信息科技有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。贵州多彩宝互联网服务有限公司、联想集团、山东云天安全技术有限公司、北京信联科汇科技有限公司、河南灵创电子科技有限公司、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、长春嘉诚信息技术股份有限公司、杭州海康威视数字技术股份有限公司、南京树安信息技术有限公司、浙江木链物联网科技有限公司、福建省海峡信息技术有限公司、北京安帝科技有限公司、杭州迪普科技股份有限公司、内蒙古云科数据服务股份有限公司、内蒙古洞明科技有限公司、南京众智维信息科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京山石网科信息技术有限公司、北京华云安信息技术有限公司、重庆都会信息科技、北京网御星云信息技术有限公司、河南信安世纪科技有限公司、安元实验室、苏州棱镜七彩信息科技有限公司、北京美亚柏科网络安全科技有限公司、奇安信-工控安全实验室、百度在线网络技术有限公司、中移（杭州）信息技术有限公司、腾讯安全天马实验室、四川博恩信息技术有限公司、深圳市魔方安全科技有限公司、北京水木羽林科技有限公司、思而听网络科技有限公司、杭州天谷信息科技有限公司、北京机沃科技有限公司、山石网科通信技术股份有限公司、广州安亿信软件科技有限公司、郑州天宇鸿图电子科技有限公司、安徽长泰科技有限公司、云南南天电子信息产业股份有限公司、华泰人寿保险股份有限公司、北方实验室（沈阳）股份有限公司、苏州棱镜七彩信息科技有限公司、中国银河证券股份有限公司、天讯瑞达通信技术有限公司及其他个人白帽子向 CNVD 提交了 20493 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 17506 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） | 13091 | 13091 |

| | | |
|---|---|---|
| 斗象科技（漏洞盒子） | 3910 | 3910 |
| 上海交大 | 505 | 505 |
| 北京奇虎科技有限公司 | 400 | 0 |
| 新华三技术有限公司 | 285 | 0 |
| 哈尔滨安天科技集团股份有限公司 | 248 | 0 |
| 厦门服云信息科技有限公司 | 225 | 0 |
| 北京神州绿盟科技有限公司 | 215 | 9 |
| 北京数字观星科技有限公司 | 199 | 0 |
| 恒安嘉新(北京)科技股份公司 | 150 | 0 |
| 北京华顺信安科技有限公司 | 127 | 0 |
| 华为技术有限公司 | 112 | 0 |
| 深信服科技股份有限公司 | 111 | 0 |
| 北京启明星辰信息安全技术有限公司 | 64 | 3 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 64 | 64 |
| 天津市国瑞数码安全系统股份有限公司 | 59 | 0 |
| 北京天融信网络安全技术有限公司 | 38 | 38 |
| 卫士通信息产业股份有限公司 | 13 | 13 |
| 南京联成科技发展股份有限公司 | 9 | 9 |
| 杭州安恒信息技术股 | 8 | 8 |

| | | |
|---|---|---|
| 份有限公司 | | |
| 北京知道创宇信息技术有限公司 | 2 | 0 |
| 浙江大华技术股份有限公司 | 2 | 2 |
| 中兴通讯股份有限公司 | 1 | 1 |
| 沈阳东软系统集成工程有限公司 | 1 | 1 |
| 贵州多彩宝互联网服务有限公司 | 477 | 477 |
| 联想集团 | 193 | 1 |
| 山东云天安全技术有限公司 | 157 | 157 |
| 北京信联科汇科技有限公司 | 133 | 133 |
| 河南灵创电子科技有限公司 | 106 | 106 |
| 广东蓝爵网络安全技术股份有限公司 | 95 | 95 |
| 新疆海狼科技有限公司 | 75 | 75 |
| 长春嘉诚信息技术股份有限公司 | 65 | 65 |
| 杭州海康威视数字技术股份有限公司 | 62 | 62 |
| 南京树安信息技术有限公司 | 32 | 32 |
| 浙江木链物联网科技有限公司 | 30 | 30 |
| 福建省海峡信息技术有限公司 | 26 | 26 |
| 北京安帝科技有限公司 | 25 | 25 |

| | | |
|---|---|---|
| 亚信科技（成都）有限公司 | 18 | 0 |
| 杭州迪普科技股份有限公司 | 17 | 3 |
| 内蒙古云科数据服务股份有限公司 | 14 | 14 |
| 内蒙古洞明科技有限公司 | 12 | 12 |
| 南京众智维信息科技有限公司 | 10 | 10 |
| 北京云科安信科技有限公司（Seraph 安全实验室） | 10 | 10 |
| 北京山石网科信息技术有限公司 | 10 | 10 |
| 北京华云安信息技术有限公司 | 9 | 9 |
| 重庆都会信息科技 | 8 | 8 |
| 北京网御星云信息技术有限公司 | 7 | 7 |
| 河南信安世纪科技有限公司 | 6 | 6 |
| 安元实验室 | 3 | 3 |
| 苏州棱镜七彩信息科技有限公司 | 2 | 2 |
| 北京美亚柏科网络安全科技有限公司 | 2 | 2 |
| 奇安信-工控安全实验室 | 2 | 2 |
| 百度在线网络技术有限公司 | 2 | 2 |
| 中移（杭州）信息技术有限公司 | 1 | 1 |
| 腾讯安全天马实验室 | 1 | 1 |

| | | |
|---|---|---|
| 四川博恩信息技术有限公司 | 1 | 1 |
| 深圳市魔方安全科技有限公司 | 1 | 1 |
| 北京水木羽林科技有限公司 | 1 | 1 |
| 思而听网络科技有限公司 | 1 | 1 |
| 杭州天谷信息科技有限公司 | 1 | 1 |
| 北京机沃科技有限公司 | 1 | 1 |
| 山石网科通信技术股份有限公司 | 1 | 1 |
| 广州安亿信软件科技有限公司 | 1 | 1 |
| 郑州天宇鸿图电子科技有限公司 | 1 | 1 |
| 安徽长泰科技有限公司 | 1 | 1 |
| 云南南天电子信息产业股份有限公司 | 1 | 1 |
| 华泰人寿保险股份有限公司 | 1 | 1 |
| 北方实验室（沈阳）股份有限公司 | 1 | 1 |
| 苏州棱镜七彩信息科技有限公司 | 1 | 1 |
| 中国银河证券股份有限公司 | 1 | 1 |
| 天讯瑞达通信技术有限公司 | 1 | 1 |
| CNCERT 贵州分中心 | 6 | 6 |
| CNCERT 四川分中心 | 5 | 5 |

| | | |
|---|---|---|
| CNCERT 青海分中心 | 5 | 5 |
| CNCERT 河北分中心 | 3 | 3 |
| CNCERT 宁夏分中心 | 1 | 1 |
| 个人 | 1417 | 1417 |
| 报送总计 | 22902 | 20493 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 484 个漏洞。智能设备（物联网终端设备）159 个， WEB 应用 138 个，应用程序 79 个，网络设备（交换机、路由器等网络端设备）45 个，操作系统 43 个，安全产品 18 个，数据库 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 |
|---|---|
| 智能设备（物联网终端设备） | 159 |
| WEB 应用 | 138 |
| 应用程序 | 79 |
| 网络设备（交换机、路由器等网络端设备） | 45 |
| 操作系统 | 43 |
| 安全产品 | 18 |
| 数据库 | 2 |

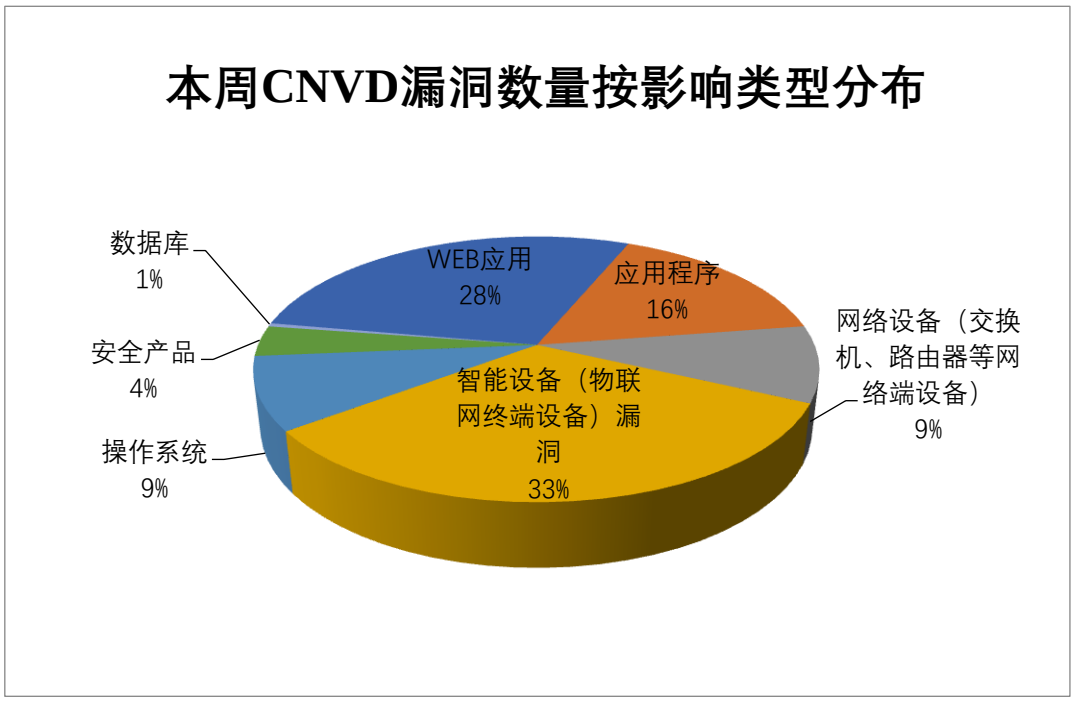


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Huawei、Google、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 | Huawei | 37 | 8% |
| 2 | Google | 32 | 7% |
| 3 | IBM | 21 | 4% |
| 4 | Mozilla | 20 | 4% |
| 5 | TOTOLINK | 15 | 3% |
| 6 | 惠普贸易（上海）有限公司 | 14 | 3% |
| 7 | Adobe | 14 | 3% |
| 8 | Delta Electronics | 10 | 2% |
| 9 | 廊坊市极致网络科技有限公司 | 7 | 1% |
| 10 | 其他 | 314 | 65% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，30 个移动互联网行业漏洞，20 个工控行业漏洞（如下图所示）。其中，“Huawei Emui 和 Magic UI 内存访问越界漏洞、Huawei Emui 和 Magic UI 劫持未经验证提供商漏洞”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/

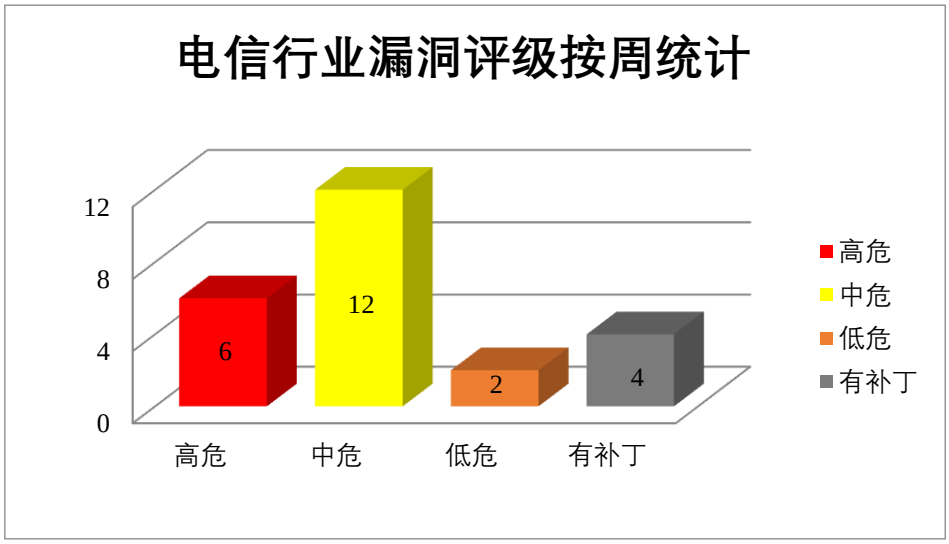


图 3 电信行业漏洞统计

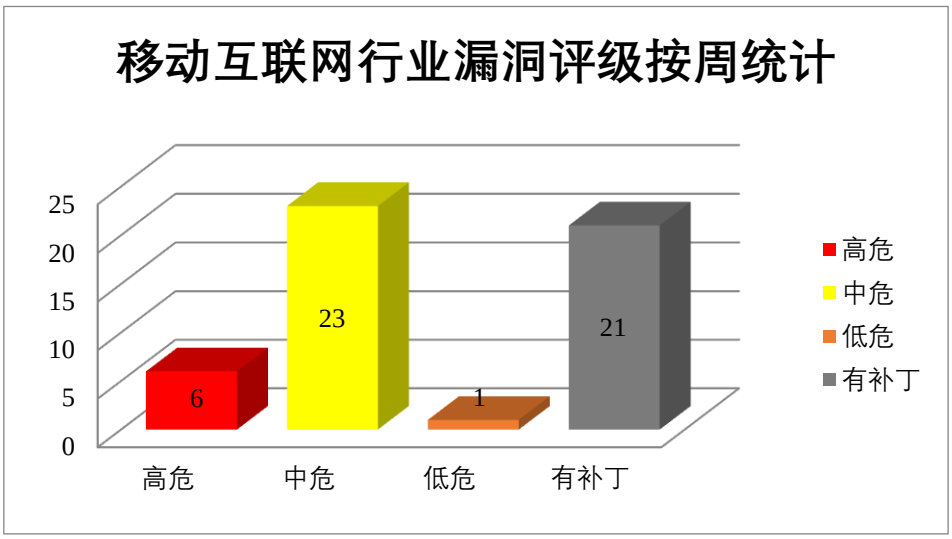


图 4 移动互联网行业漏洞统计

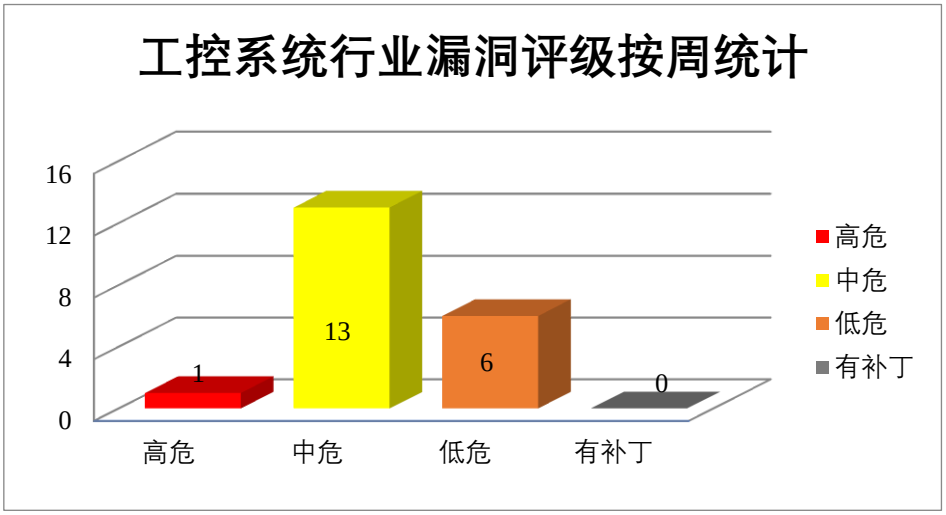


图 5 工控系统行业漏洞统计

## 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、 IBM 产品安全漏洞

IBM InfoSphere Information Server 是一个数据集成平台，包含一系列产品，使您能够理解、清理、监控、转换及传送数据，以及协作以弥合业务与 IT 之间的差距。Ibm InfoSphere DataStage Flow Designer 是美国 Ibm 公司的一个基于 Web 的数据阶段流程设计器。IBM Cognos Analytics 是美国 IBM 公司的一套商业智能软件，可提供有价值的信息、安全的数据治理和报告。IBM Security Guardium 是美国 IBM 公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。IBM Sterling B2B Integrator 是美国 IBM 公司的一套集成了重要的 B2B 流程、交易和关系的软件。该软件支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安

全集成。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受影响组件敏感信息，非法执行 SQL 命令窃取数据库敏感数据，越权访问”新作业”页面，远程执行代码等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2021-87010）、IBM Planning Analytics 信息泄露漏洞（CNVD-2021-87013）、IBM InfoSphere DataStage Flow Designer 代码问题漏洞、IBM Sterling B2B Integrator 授权问题漏洞（CNVD-2021-87017）、IBM Cognos Analytics 权限提升漏洞（CNVD-2021-87015）、IBM Cognos Analytics 远程代码执行漏洞、IBM Security Guardium 硬编码凭证漏洞、IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2021-87020）。其中“IBM Security Guardium 硬编码凭证漏洞、IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2021-87020）”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-2021-87010
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87013
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87012
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87017
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87015
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87014
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87021
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87020

## 2、Huawei 产品安全漏洞

Huawei Emui 是一款基于 Android 开发的移动端操作系统。Magic Ui 是一款基于 Android 开发的移动端操作系统。Huawei FusionCompute 是中国华为（Huawei）公司的一款计算机虚拟化引擎。该产品提供虚拟资源管理器（VRM）和计算节点代理（CNA）等。Huawei AIS-BW50-00 是中国华为（Huawei）公司的一款便携式蓝牙音箱。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致进程异常，劫持设备并伪造 UI 诱使用户执行恶意命令，在特定场景下处理证书文件时进行命令注入，在目标设备中执行任意代码等。

CNVD 收录的相关漏洞包括：Huawei Emui 和 Magic UI 远程 DoS 漏洞（CNVD-2021-84859）、Huawei Emui 和 Magic UI 配置缺陷漏洞（CNVD-2021-84858、CNVD-2021-84860）、Huawei Emui 和 Magic UI 目录遍历漏洞、Huawei Emui 和 Magic UI 内存访问越界漏洞、Huawei Emui 和 Magic UI 劫持未经验证提供商漏洞、Huawei FusionCompute 命令注入漏洞（CNVD-2021-84882）、Huawei AIS-BW50-00 授权问题漏洞。其中“Huawei Emui 和 Magic UI 内存访问越界漏洞、Huawei Emui 和 Magic UI 劫持未经验证提供商漏洞、Huawei FusionCompute 命令注入漏洞（CNVD-2021-84882）、H

uawei AIS-BW50-00 授权问题漏洞”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-2021-84860
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84859
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84858
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84857
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84869
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84877
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84882
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84884

### 3、Mozilla 产品安全漏洞

Rust 是 Mozilla 基金会的一款通用、编译型编程语言。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞创建释放后使用访问，导致并发程序中的数据竞争的错误，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Mozilla Rust 资源管理错误漏洞（CNVD-2021-85285、CNVD-2021-85301）、Mozilla Rust 内存损坏漏洞、Mozilla Rust 命令注入漏洞（CNVD-2021-85287）、Mozilla Rust 缓冲区溢出漏洞（CNVD-2021-85300、CNVD-2021-85299、CNVD-2021-85298、CNVD-2021-85297、）。其中“Mozilla Rust 资源管理错误漏洞（CNVD-2021-85301）”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-2021-85285
https://www.cnvd.org.cn/flaw/show/CNVD-2021-85284
https://www.cnvd.org.cn/flaw/show/CNVD-2021-85287
https://www.cnvd.org.cn/flaw/show/CNVD-2021-85300
https://www.cnvd.org.cn/flaw/show/CNVD-2021-85299
https://www.cnvd.org.cn/flaw/show/CNVD-2021-85298
https://www.cnvd.org.cn/flaw/show/CNVD-2021-85297
https://www.cnvd.org.cn/flaw/show/CNVD-2021-85301

### 4、Google 产品安全漏洞

Chrome 是由 Google 开发的一款 Web 浏览工具。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞获取数据库敏感信息，导致程序崩溃或者拒绝服务等。

CNVD 收录的相关漏洞包括：Google Chrome 输入验证不足漏洞（CNVD-2021-84801）、Google Chrome WebApp Installer 实现不当漏洞、Google Chrome 释放后重用漏洞（CNVD-2021-84803、CNVD-2021-84808）、Google Chrome iFrame Sandbox 实现不

当漏洞、Google Chrome 竞争条件漏洞（CNVD-2021-84805）、Google Chrome 越界读取漏洞（CNVD-2021-84804）、Google Chrome Blink 实现不当漏洞（CNVD-2021-84806）。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-2021-84801
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84800
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84803
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84802
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84805
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84804
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84806
https://www.cnvd.org.cn/flaw/show/CNVD-2021-84808

### 5、D-Link DIR-823G 命令注入漏洞（CNVD-2021-85889）

D-Link DIR-823G 是一款 AC1200M 双频千兆无线路由器。本周，DIR-823G 被披露存在命令注入漏洞。攻击者可通过登录部分的 Captcha 字段中的 shell 元字符利用该漏洞执行任意 Web 脚本。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-2021-85889

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-2021-85251 | TOTOLINK EX200 存在命令执行漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：http://totolink.net/ |
| CNVD-2021-84825 | Apache Traffic Server 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://lists.apache.org/thread/k01797hyncx53659wr3o72s5cvkc3164 |
| CNVD-2021-85265 | Adobe InDesign 缓冲区溢出漏洞（CNVD-2021-85265） | 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/indesign/apsb21-107.html |
| CNVD-2021-85269 | Adobe InDesign 越界读取漏洞 | 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/indesign/apsb21-73.html |
| CNVD-2021 | Adobe InDesign 越界读取漏 | 高 | 厂商已发布了漏洞修复程序，请及 |

| | | | |
|---|---|---|---|
| -85268 | 洞（CNVD-2021-85268） | | 时关注更新：https://helpx.adobe.com/security/products/indesign/apsb21-73.html |
| CNVD-2021-85266 | Adobe InDesign 内存缓冲区越界访问漏洞 | 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/indesign/apsb21-107.html |
| CNVD-2021-85270 | Adobe InDesign 内存越界访问漏洞 | 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/indesign/apsb21-73.html |
| CNVD-2021-85301 | Mozilla Rust 资源管理错误漏洞（CNVD-2021-85301） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://rustsec.org/advisories/RUSTSEC-2020-0100.html |
| CNVD-2021-87021 | IBM Security Guardium 硬编码凭证漏洞 | 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/6491125 |
| CNVD-2021-87041 | Linux kernel 输入验证错误漏洞（CNVD-2021-87041） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.14.16。 |

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用该漏洞获取受影响组件敏感信息，非法执行 SQL 命令窃取数据库敏感数据，越权访问“新作业”页面，远程执行代码等。此外，Huawei、Mozilla、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致进程异常，劫持设备并伪造 UI 诱使用户执行恶意命令，在特定场景下处理证书文件时进行命令注入，在目标设备中执行任意代码，获取数据库敏感信息，导致程序崩溃或者拒绝服务等。另外，D-Link DIR-823G 被披露存在命令注入漏洞。攻击者可通过登录部分的 Captcha 字段中的 shell 元字符利用该漏洞执行任意 Web 脚本。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、webTareas 跨站脚本漏洞

**验证描述**

webTareas 是一款基于 Web 的开源协作工具。该产品支持项目管理、错误跟踪、内容管理和会议管理等功能。

webTareas 2.0p8 版本中 general/login.php 网页中的 loginForm 存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端

代码。

**验证信息**

POC 链接：https://packetstormsecurity.com/files/157608/WebTareas-2.0p8-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-85281

**信息提供者**

恒安嘉新(北京)科技股份公司

*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. 黑客利用 macOS 零日漏洞攻击香港用户

谷歌安全研究员透露，8 月下旬，黑客利用 macOS 零日漏洞，攻击了一家香港网站。

参考链接：https://thehackernews.com/2021/11/hackers-exploit-macos-zero-day-to-hack.html

### 2. Lyceum 黑客组织将以色列、沙特阿拉伯等国的电信运营商锁定为攻击目标

据称国家资助的威胁行为者针对以色列、摩洛哥、突尼斯和沙特阿拉伯等国的互联网服务提供商 (ISP) 和电信运营商开展了一系列网络攻击。

参考链接：https://thehackernews.com/2021/11/irans-lyceum-hackers-target-telecoms.html

**关于 CNVD**

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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