

## 信息安全漏洞周报

2023年09月18日-2023年09月24日

2023年第38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 69 个，其中高危漏洞 145 个、中危漏洞 205 个、低危漏洞 19 个。漏洞平均分为 6.30。本周收录的漏洞中，涉及 0day 漏洞 306 个（占 83%），其中互联网上出现“JFinalCMS 目录遍历漏洞、WordPress Leyka plugin 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 17693 个，与上周（8319 个）环比增加 1.13 倍。

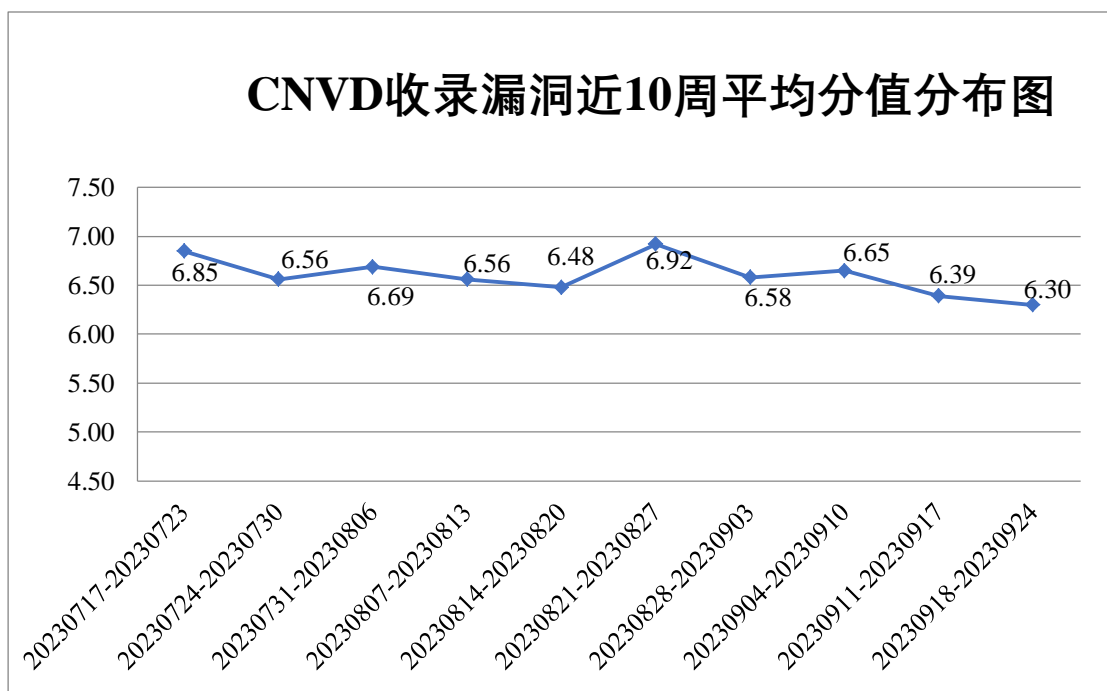


图 1 CNVD 收录漏洞近 10 周平均分分布图

### 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 26 起，向基础电

信企业通报漏洞事件 12 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 967 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 134 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 39 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、重庆米未科技有限公司、中山佳维电子有限公司、中企动力科技股份有限公司、中海创科技（福建）集团有限公司、智联招聘、郑州大象通信信息技术有限公司、浙江中控技术股份有限公司、浙江星汉信息技术股份有限公司、浙江新奥电梯有限公司、浙江深大智能集团、浙江兰德纵横网络技术股份有限公司、长沙市业通达监控技术有限公司、云程科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、用友金融信息技术股份有限公司、夏普商贸（中国）有限公司、西安众邦网络科技有限公司、西安信步电子信息技术有限公司、西安悟空检测科技有限公司、西安沃户时间区块链科技股份有限公司、西安瑞友信息技术资讯有限公司、西安恒谦教育科技股份有限公司、武汉云水网络科技有限公司、武汉深之度科技有限公司、武汉理工光科股份有限公司、武汉华信数据系统有限公司、武汉海创华联信息技术有限公司、武汉达梦数据库有限公司、无锡骑行联盟科技有限公司、潍坊家园驿站电子技术有限公司、微客新媒体科技(重庆)有限公司、网是科技股份有限公司、崑远科技股份有限公司、统信软件技术有限公司、天津海厚科技发展有限公司、天地伟业技术有限公司、特斯拉（上海）有限公司、泰华智慧产业集团股份有限公司、太原易思软件技术有限公司、台达电子企业管理（上海）有限公司、苏州赏聘网络科技有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、首辅工程设计有限公司、世邦通信股份有限公司、神州数码集团股份有限公司、深圳智慧光迅信息技术有限公司、深圳维盟科技股份有限公司、深圳市中科网威科技有限公司、深圳市万网博通科技有限公司、深圳市深度网络有限公司、深圳市锐明技术股份有限公司、深圳市龙信信息技术有限公司、深圳市联天通信技术有限公司、深圳市科荣软件股份有限公司、深圳市捷道智控实业有限公司、深圳市吉祥腾达科技有限公司、深圳市电航科技发展有限公司、深圳市博思协创网络科技有限公司、深圳市昂捷信息技术股份有限公司、深圳市爱德数智科技股份有限公司、深信服科技股份有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海装盟信息科技有限公司、上海蒜芽信息科技有限公司、上海商创网络科技有限公司、上海穆云智能科技有限公司、上海华测导航技术股份有限公司、上海斐讯数据通信技术有限公司、上海顶想信息科技有限公司、上海博达数据通信有限公司、上海艾泰科技有限公司、陕西凯星电子科技有限公司、陕西法华网络科技有限公司、陕西诚义信科技有限公司、山西青峰软件股份有限公司、山脉科技股份有限公司、山东中创软件商用中间件股份有限公司、山东大有医网医疗科

技术有限公司、山东博硕自动化技术有限公司、厦门亿联网络技术股份有限公司、厦门睿天科技有限公司、厦门安贸通科技有限公司、锐捷网络股份有限公司、任子行网络技术股份有限公司、青岛雨诺网络信息股份有限公司、麒麟软件有限公司、普联技术有限公司、南宁红树林软件技术有限公司、南都物业服务集团股份有限公司、辽宁云盾网力科技有限公司、力合科技（湖南）股份有限公司、廊坊市极致网络科技有限公司、蓝网科技股份有限公司、昆山双叶软件科技有限公司、金蝶天燕云计算股份有限公司、江西登云健康美业互联有限公司、江苏省广电有线信息网络股份有限公司、嘉兴想天信息科技有限公司、吉翁电子（深圳）有限公司、基恩士（中国）有限公司、惠普贸易（上海）有限公司、湖南赛吉智慧城市建设管理有限公司、湖南强智科技发展有限公司、杭州易软共创网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州新视窗信息技术有限公司、杭州商计科技有限公司、杭州三汇信息工程有限公司、杭州吉拉科技有限公司、杭州宏服软件有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、杭州安猫区块链科技有限公司、汉王科技股份有限公司、海南链盒科技有限公司、贵派电器股份有限公司、广州易全信息科技有限公司、广州同聚成电子科技有限公司、广州红帆科技有限公司、广联达科技股份有限公司、广东振丰科教玩具有限公司、广东世季科技有限公司、广东飞企互联科技股份有限公司、广东百沃信息技术服务有限公司、福州联讯信息科技有限公司、福建星网锐捷通讯股份有限公司、福建盟购信息科技有限公司、福建科立讯通信有限公司、成都星锐蓝海网络科技有限公司、成都任我行软件股份有限公司、畅捷通信息技术股份有限公司、彩讯科技股份有限公司、北京中科基因技术股份有限公司、北京中成科信科技发展有限公司、北京致远互联软件股份有限公司、北京用友政务软件股份有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京信达网安科技有限公司、北京通达信科科技有限公司、北京世纪明德教育科技股份有限公司、北京神州视翰科技有限公司、北京慕华信息科技有限公司、北京朗新天霁软件技术有限公司、北京快学在线教育科技有限公司、北京金水中科科技有限公司、北京金山数字娱乐科技有限公司、北京金和网络股份有限公司、北京华清信安科技有限公司、北京好运锦鲤科技有限公司、北京锋脉智软科技有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、安徽旭帆信息科技有限公司、安徽青柿信息科技有限公司和阿里巴巴集团安全应急响应中心。



## 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、新华三技术有限公司、北京启明星辰信息安全技术有限公司、北京数字观星科技有限公司、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。联想集团、奇安星城网络安全运营服务（长沙）有限公司、博智安全科技股份有限公司、亚信科技（成都）有限公

司、快页信息技术有限公司、北京中关村实验室、江苏云天网络安全技术有限公司、安徽锋刃信息科技有限公司、西藏熙安信息技术有限责任公司、中孚安全技术有限公司、中电智安科技有限公司、河南东方云盾信息技术有限公司、北京网御星云信息技术有限公司、合肥梆梆信息科技有限公司、星云博创科技有限公司、信息产业信息安全测评中心、山东云天安全技术有限公司、赛尔网络有限公司、中国电信股份有限公司上海研究院、杭州飞致云信息科技有限公司、北京君云天下科技有限公司、信联科技（南京）有限公司、北京众安天下科技有限公司、浙江中控技术股份有限公司、江苏金陵科技集团有限公司、北京威努特技术有限公司、江苏晟晖信息科技有限公司、江苏极元信息技术有限公司、云南联创网安科技有限公司、湖南泛联新安信息科技有限公司、河南灵创电子科技有限公司、杭州默安科技有限公司、平安银河实验室、北京山石网科信息技术有限公司、上海上讯信息技术股份有限公司、工业和信息化部电子第五研究所-数据治理服务中心、西安安迈信科科技有限公司、北京六方云信息技术有限公司、汇安云（山东）信息科技有限公司、雅信科技、北京墨云科技有限公司、成都安美勤信息技术股份有限公司、北京安帝科技有限公司、国网江西省电力有限公司电力科学研究院、北京天防安全科技有限公司、河南悦海数安科技有限公司、上海观安信息技术股份有限公司、杭州中正检测技术有限公司、广州安亿信软件科技有限公司及其他个人白帽子向 CNVD 提交了 17693 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、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 15270 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)	8288	8288
奇安信网神(补天平台)	6336	6336
北京天融信网络安全技术有限公司	501	0
上海交大	498	498
新华三技术有限公司	458	0
北京启明星辰信息安全技术有限公司	435	12
北京数字观星科技有限公司	425	0
北京神州绿盟科技有限公司	404	1
天津市国瑞数码安全	296	0

系统股份有限公司		
安天科技集团股份有 限公司	250	3
三六零数字安全科技 集团有限公司	148	148
深信服科技股份有限 公司	82	0
北京知道创宇信息技 术有限公司	60	0
北京长亭科技有限公 司	56	1
杭州安恒信息技术股 份有限公司	46	0
杭州迪普科技股份有 限公司	25	0
中电科网络安全科技 股份有限公司	15	15
南京联成科技发展股 份有限公司	12	12
中国电信股份有限公 司网络安全产品运营 中心	7	7
阿里云计算有限公司	6	6
深圳市腾讯计算机系 统有限公司（玄武实 验室）	2	2
北京智游网安科技有 限公司	1	1
远江盛邦（北京）网 络安全科技股份有限 公司	1	1
北京信联数安科技有 限公司	1	1
浙江大华技术股份有 限公司	1	1

联想集团	100	100
奇安信网络安全运营服务（长沙）有限公司	71	71
博智安全科技股份有限公司	70	70
亚信科技（成都）有限公司	38	37
快页信息技术有限公司	26	26
北京中关村实验室	18	18
江苏云天网络安全技术有限公司	15	15
安徽锋刃信息科技有限公司	14	14
西藏熙安信息技术有限责任公司	13	13
中孚安全技术有限公司	10	10
中电智安科技有限公司	9	9
河南东方云盾信息技术有限公司	9	9
北京网御星云信息技术有限公司	8	8
合肥梆梆信息科技有限公司	7	7
星云博创科技有限公司	7	7
信息产业信息安全测评中心	6	6
山东云天安全技术有限公司	5	5
赛尔网络有限公司	4	4
中国电信股份有限公司	4	4

司上海研究院		
杭州飞致云信息科技有限公司	3	3
北京君云天下科技有限公司	3	3
信联科技（南京）有限公司	3	3
北京众安天下科技有限公司	3	3
浙江中控技术股份有限公司	2	2
江苏金陵科技集团有限公司	2	2
北京威努特技术有限公司	2	2
江苏晟晖信息科技有限公司	2	2
江苏极元信息技术有限公司	2	2
云南联创网安科技有限公司	2	2
湖南泛联新安信息科技有限公司	2	2
河南灵创电子科技有限公司	2	2
杭州默安科技有限公司	2	2
平安银河实验室	1	1
北京山石网科信息技术有限公司	1	1
上海上讯信息技术股份有限公司	1	1
工业和信息化部电子第五研究所-数据治理服务中心	1	1

西安安迈信科科技有限公司	1	1
北京六方云信息技术有限公司	1	1
汇安云（山东）信息科技有限公司	1	1
雅信科技	1	1
北京墨云科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
北京安帝科技有限公司	1	1
国网江西省电力有限公司电力科学研究院	1	1
北京天防安全科技有限公司	1	1
河南悦海数安科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
杭州中正检测技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
CNCERT 河北分中心	2	2
个人	1878	1878
报送总计	20715	17693

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 369 个漏洞。WEB 应用 191 个，应用程序 97 个，网络设备（交换机、路由器等网络端设备）35 个，操作系统 24 个，安全产品 11 个，数据库 6 个，智能设备（物联网终端设备）5 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	191
应用程序	97
网络设备（交换机、路由器等网络端设备）	35
操作系统	24
安全产品	11
数据库	6
智能设备（物联网终端设备）	5

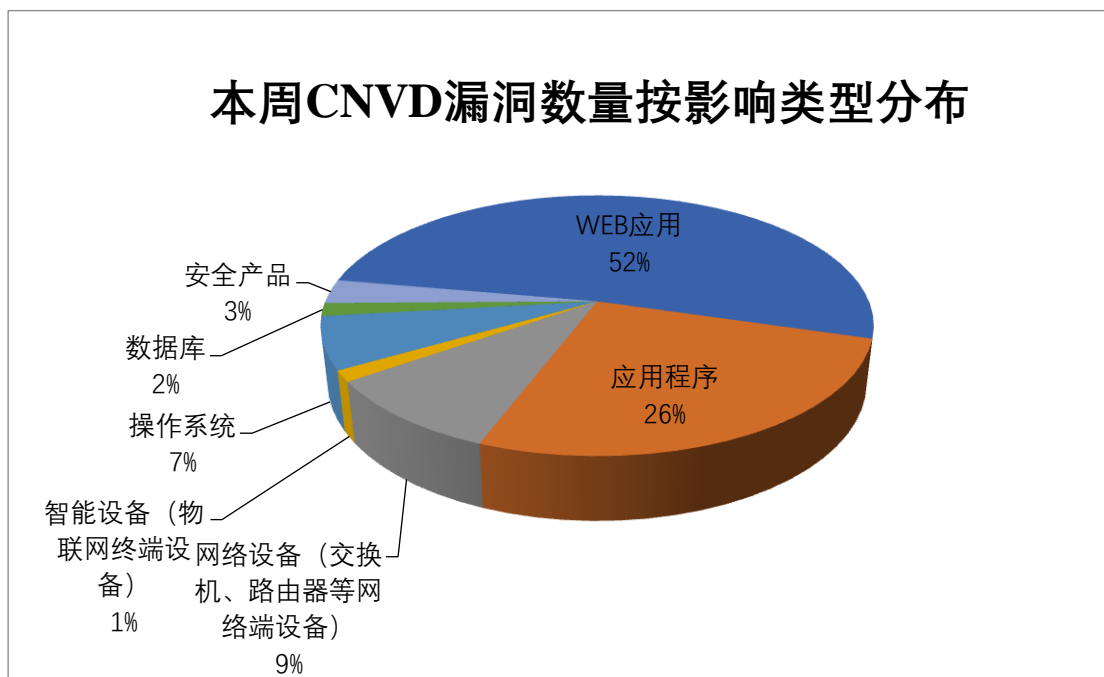


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Apache、Linux 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	14	4%
2	Apache	11	3%
3	Linux	10	2%
4	Huawei	10	2%
5	友讯电子设备（上海）有限公司	7	2%
6	Oracle	6	2%
7	用友网络科技股份有限公司	6	2%
8	北京百卓网络技术有限公司	6	2%

	司		
9	北京香哈网络股份有限公司	5	1%
10	其他	294	80%

## 本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，70 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“ASUS RT-AC86U 命令注入漏洞（CNVD-2023-70091）、Oracle Database Server 安全绕过漏洞”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/>

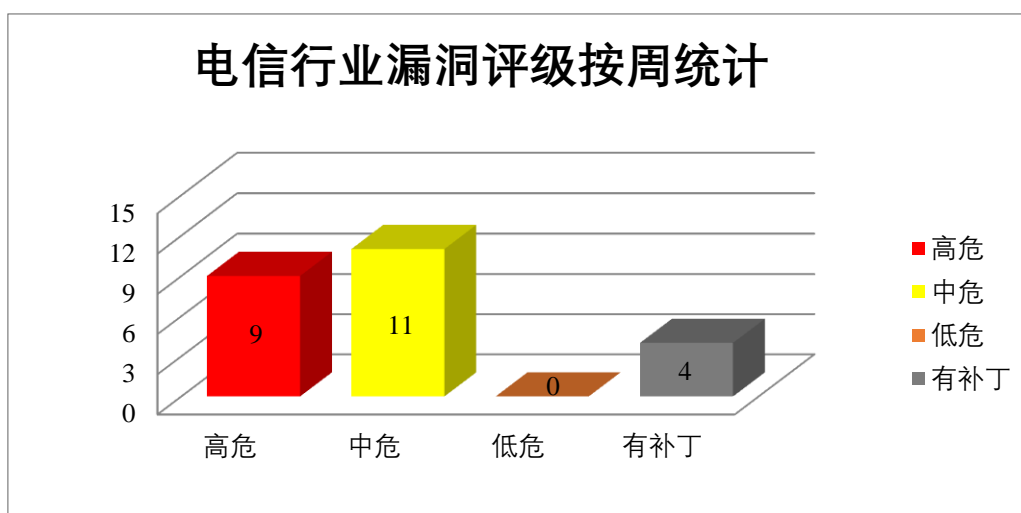


图3 电信行业漏洞统计

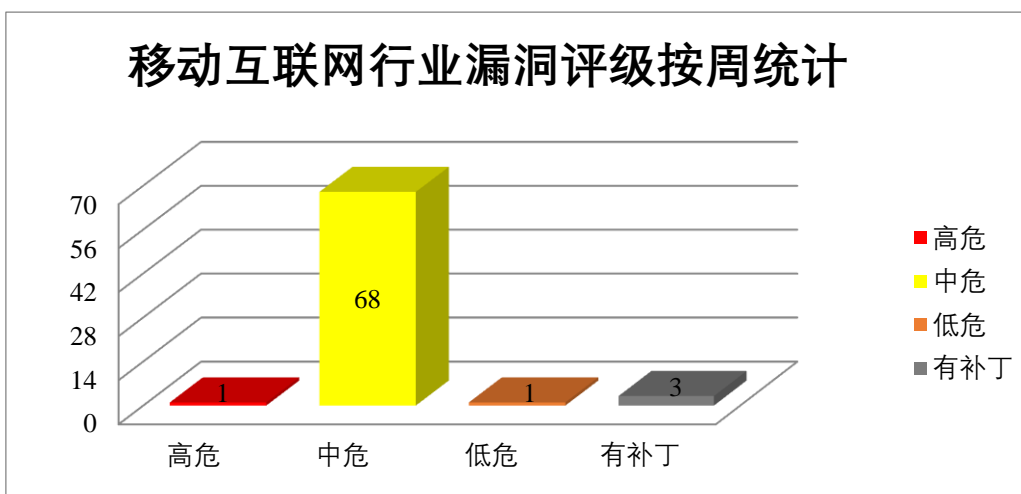


图4 移动互联网行业漏洞统计

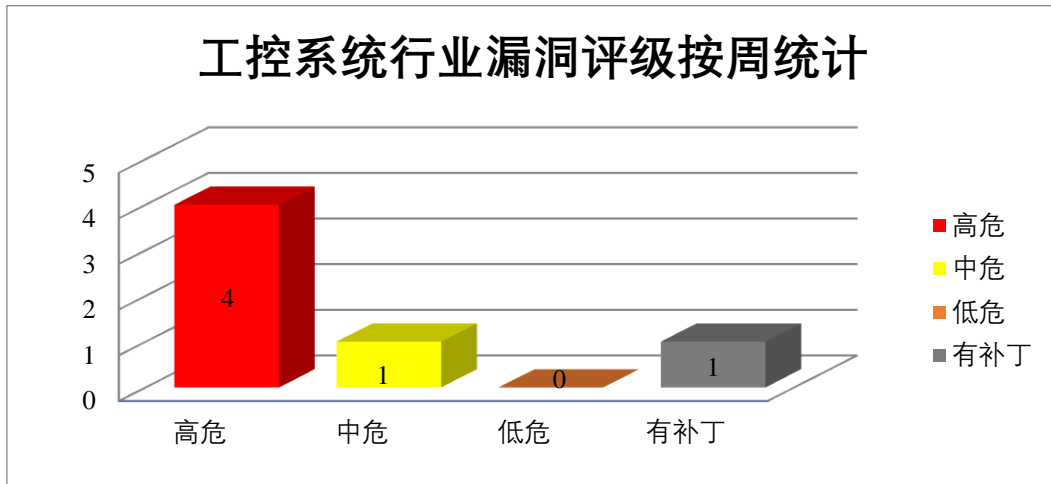


图 5 工控系统行业漏洞统计

## 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、Siemens 产品安全漏洞

Siemens QMS Automotive 是德国西门子（Siemens）公司的一个汽车行业的质量管理系统。Siemens Tecnomatix Plant Simulation 是工控设备，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。Siemens Solid Edge 是一款三维 CAD 软件。该软件可用于零件设计、装配设计、钣金设计、焊接设计等行业。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数据库，篡改应用程序代码，上传恶意文件，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 QMS Automotive 访问控制错误漏洞、Siemens QMS Automotive 代码问题漏洞、Siemens QMS Automotive 信息泄露漏洞（CNVD-2023-71222）、Siemens QMS Automotive 数据伪造问题漏洞、Siemens Tecnomatix Plant Simulation 缓冲区溢出漏洞、Siemens Solid Edge 内存错误引用漏洞（CNVD-2023-71238）、Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-71239、CNVD-2023-71240）。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-2023-71218>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71217>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71222>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71221>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71231>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71238>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71239>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71240>

## 2、Huawei 产品安全漏洞

Huawei HarmonyOS 是中国华为（Huawei）公司的一个基于微内核的全场景分布式操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过授权并获得访问权限，发送特制的请求，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei HarmonyOS 安全限制绕过漏洞（CNVD-2023-70288、CNVD-2023-70287、CNVD-2023-70286）、Huawei HarmonyOS 权限提升漏洞（CNVD-2023-70290）、Huawei HarmonyOS 拒绝服务漏洞（CNVD-2023-70294、CNVD-2023-70293、CNVD-2023-70292、CNVD-2023-70285）。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-2023-70285>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70288>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70287>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70286>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70290>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70294>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70293>

<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70292>

## 3、Apache 产品安全漏洞

Apache Superset 是一款由 Python 语言为主开发的开源时髦数据探索分析以及可视化的报表平台，支持丰富的数据源，且拥有多姿多彩的可视化图表选择。Apache Axis 是一个开源、基于 XML 的 Web 服务架构。该产品包含了 Java 和 C++ 语言实现的 SOAP 服务器，以及各种公用服务及 API，以生成和部署 Web 服务应用。Apache InLong 是一站式的海量数据集成框架。提供自动化、安全、可靠的数据传输能力。Apache Airflow 是一套用于创建、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。Apache RocketMQ 是一款轻量级的数据处理平台和消息传递引擎。Apache Jena 是一个 Java 语义网框架。用于构建语义 Web 和链接数据应用程序。Apache Shiro 是一套用于执行认证、授权、加密和会话管理的 Java 安全框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过当前逻辑读取任意文件，获取敏感信息，通过连接传递参数实施远程代码执行攻击，从而获取服务器权限等。

CNVD 收录的相关漏洞包括：Apache Superset 未授权访问漏洞、Apache Axis 输入验证错误漏洞、Apache InLong 反序列化漏洞（CNVD-2023-70280）、Apache Airflow 访问控制错误漏洞（CNVD-2023-70279）、Apache Airflow 输入验证错误漏洞（CNVD-2023-70278）、Apache RocketMQ 代码注入漏洞、Apache Jena 代码执行漏洞、Apach

e Shiro 路径遍历漏洞。其中，除“Apache Superset 未授权访问漏洞”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-2023-70277>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70275>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70280>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70279>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70278>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70283>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70282>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70281>

#### 4、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，攻击者可利用漏洞导致本地权限提升，获取系统上的高级权限。

CNVD 收录的相关漏洞包括：Linux kernel 权限提升漏洞（CNVD-2023-70080、CNVD-2023-70079、CNVD-2023-70083、CNVD-2023-70082、CNVD-2023-70081、CNVD-2023-70086、CNVD-2023-70085、CNVD-2023-70084）。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-2023-70080>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70079>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70083>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70082>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70081>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70086>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70085>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2023-70084>

#### 5、ASUS RT-AX55 命令注入漏洞

ASUS RT-AX55 是中国华硕（ASUS）公司的一款双频 Wi-Fi 路由器。本周，ASUS RT-AX55 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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-2023-70089>

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-2023-70289	Huawei HarmonyOS 安全限制绕过漏洞 (CNVD-2023-70289)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202308-0000001667644725">https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202308-0000001667644725</a>
CNVD-2023-71680	Google Chrome 缓冲区溢出漏洞 (CNVD-2023-71680)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html">https://chromereleases.googleblog.com/2023/09/stable-channel-update-for-desktop_11.html</a>
CNVD-2023-70279	Apache Airflow 访问控制错误漏洞 (CNVD-2023-70279)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://lists.apache.org/thread/9rdmv8ln4y4ncbyrlmjrj903x4l80nj">https://lists.apache.org/thread/9rdmv8ln4y4ncbyrlmjrj903x4l80nj</a>
CNVD-2023-70278	Apache Airflow 输入验证错误漏洞 (CNVD-2023-70278)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://lists.apache.org/thread/lswlxf11do51ob7f6xyyg8qp3n7wdrgd">https://lists.apache.org/thread/lswlxf11do51ob7f6xyyg8qp3n7wdrgd</a>
CNVD-2023-70283	Apache RocketMQ 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: <a href="https://lists.apache.org/thread/m614czxtpvlztd7mfgcs2xcsg36rdbnc">https://lists.apache.org/thread/m614czxtpvlztd7mfgcs2xcsg36rdbnc</a>
CNVD-2023-70294	Huawei HarmonyOS 拒绝服务漏洞 (CNVD-2023-70294)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202308-0000001667644725">https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202308-0000001667644725</a>
CNVD-2023-70293	Huawei HarmonyOS 拒绝服务漏洞 (CNVD-2023-70293)	高	厂商已发布了漏洞修复程序, 请及时关注更新: <a href="https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202308-0000001667644725">https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202308-0000001667644725</a>
CNVD-2023-71218	Siemens QMS Automotive 访问控制错误漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: <a href="https://cert-portal.siemens.com/productcert/html/ssa-147266.html">https://cert-portal.siemens.com/productcert/html/ssa-147266.html</a>
CNVD-2023-71217	Siemens QMS Automotive 代码问题漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: <a href="https://cert-portal.siemens.com/productcert/html/ssa-147266.html">https://cert-portal.siemens.com/productcert/html/ssa-147266.html</a>

CNVD-2023-71222	Siemens QMS Automotive 信息泄露漏洞 (CNVD-2023-71222)	高	用户可参考如下供应商提供的安全公告获得补丁信息： <a href="https://cert-portal.siemens.com/productcert/html/ssa-147266.html">https://cert-portal.siemens.com/productcert/html/ssa-147266.html</a>
-----------------	---	---	---

小结：本周，Siemens 产品被披露存在多个漏洞，攻击者可利用漏洞访问数据库，篡改应用程序代码，上传恶意文件，在当前进程的上下文中执行代码等。此外，Huawei、Apache、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过当前逻辑读取任意文件，获取敏感信息，发送特制的请求，导致拒绝服务，本地权限提升等。另外，ASUS RT-AX55 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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、WordPress Leyka plugin 跨站脚本漏洞

#### 验证描述

WordPress 和 WordPress plugin 都是 WordPress 基金会的产品。WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。WordPress plugin 是一个应用插件。

WordPress Leyka plugin 3.30.3 及之前版本存在跨站脚本漏洞，该漏洞源于未清理和转义其某些设置，攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

#### 验证信息

POC 链接：<https://wpscan.com/vulnerability/762ff2ca-5c1f-49ae-b83c-1c22bacbc82f>

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2023-71325>

#### 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. 苹果更新修复了 3 个新的零日漏洞

苹果公司发布了安全更新，以修补针对 iPhone 和 Mac 用户的攻击中利用的三个新零日漏洞，今年共修复了 16 个零日漏洞。

参考链接: <https://www.bleepingcomputer.com/news/apple/apple-emergency-updates-fix-3-new-zero-days-exploited-in-attacks/>

## 2. Atlassian 产品和 ISC BIND 服务器中发现安全漏洞

Atlassian 和互联网系统联盟 (ISC) 披露了影响其产品的几个安全漏洞, 这些漏洞可能被用来实现拒绝服务 (DoS) 和远程代码执行。

参考链接: <https://thehackernews.com/2023/09/high-severity-flaws-uncovered-in.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](http://www.cert.org.cn)

邮箱: [vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话: 010-82991537