国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 09 月 11 日-2023 年 09 月 17 日 **2023 年第 37 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 437 个，其中高危漏洞 188 个、中危漏洞 227 个、低危漏洞 22 个。漏洞平均分值为 6.39。本周收录的漏洞中，涉及 0day 漏洞 363 个（占 83%），其中互联网上出现“Simple Cold Storage Management System SQL 注入漏洞（CNVD-2023-69723）、Password Storage Application 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 8319 个，与上周（16173 个）环比减少 49%。

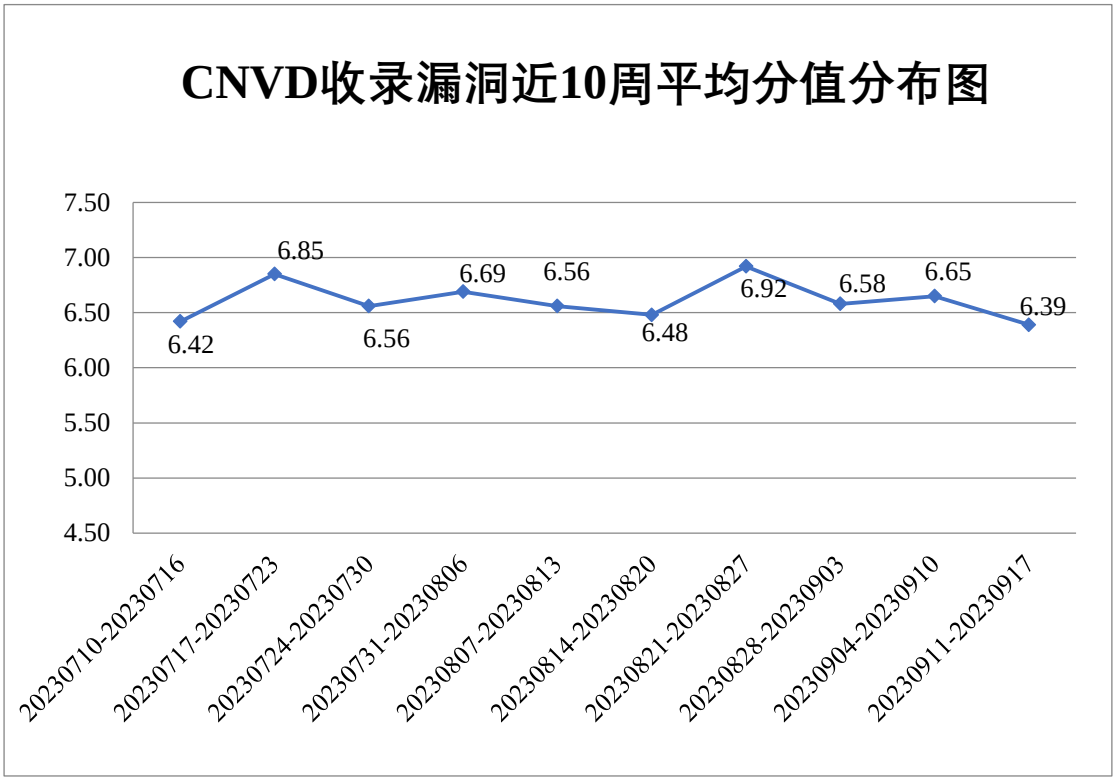

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 起，向基础电信企业通报漏洞事件 13 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 829 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 141 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 50 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、淄博闪灵网络科技有限公司、重庆中联信息产业有限责任公司、中科网威信息技术有限公司、中科方德软件有限公司、中孚信息股份有限公司、智慧芽信息科技（苏州）有限公司、智互联（深圳）科技有限公司、郑州众智科技股份有限公司、浙江云马智慧科技有限公司、浙江宇视科技有限公司、浙江清华长三角研究院、浙江励璞信息科技有限公司、浙江禾川科技股份有限公司、长沙市中智信息技术开发有限公司、长春吉大正元信息技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、宜宾北斗网络科技开发有限公司、西安紫云羚网络科技有限责任公司、西安和讯数智科技有限公司、武汉儒松科技有限公司、无锡微智格信息科技有限公司、万兴科技集团股份有限公司、崴远科技股份有限公司、同望科技股份有限公司、天津天堰科技股份有限公司、腾讯安全应急响应中心、唐山盛炜科技有限公司、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、苏州中成新能源科技股份有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、首都信息发展股份有限公司、世邦通信股份有限公司、石家庄宝智软件科技有限公司、深圳亿网云科技有限公司、深圳市西迪特科技股份有限公司、深圳市维拍物联智能技术有限公司、深圳市网力软件有限公司、深圳市天软科技开发有限公司、深圳市思迅软件股份有限公司、深圳市深日科技有限公司、深圳市龙信信息技术有限公司、深圳市揽胜科技有限公司、深圳市蓝凌软件股份有限公司、深圳市佳为软件开发有限公司、深圳市宏电技术股份有限公司、深圳市和为顺网络技术有限公司、深圳市多迪信息科技有限公司、深圳市单仁牛商科技股份有限公司、深圳市爱德数智科技股份有限公司、深圳诺普信作物科学股份有限公司、深圳警翼智能科技股份有限公司、申瓯通信设备有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海助医信息网络有限公司、上海邺嘉数字科技有限公司、上海泰宇信息技术股份有限公司、上海商创网络科技有限公司、上海企望信息科技有限公司、上海宽娱数码科技有限公司、上海寰创通信科技股份有限公司、上海覆盆子信息科技有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海必智科技有限公司、上海艾泰科技有限公司、商派软件有限公司、陕西卡一车物流科技有限公司、山西建投物资贸易有限公司、山脉科技股份有限公司、山东潍大软件有限公司、山东省诚信行物业管理有限公司、山东仁

科测控技术有限公司、山东科然信息技术有限公司、厦门一指通智能科技有限公司、厦门星纵物联科技有限公司、厦门四信通信科技有限公司、融智通科技（北京）股份有限公司、任子行网络技术股份有限公司、清远市帕克文化传媒有限公司、青岛海信网络科技股份有限公司、普联技术有限公司、欧姆龙自动化（中国）有限公司、南京悠珀网络科技有限公司、南京英安特科技实业有限公司、南京特临信息科技有限公司、南京南瑞信息通信科技有限公司、南京爱普雷德电子科技有限公司、牦牛信息科技（杭州）有限公司、迈普通信技术股份有限公司、联奕科技股份有限公司、联想集团、连云港信友科技有限公司、朗坤智慧科技股份有限公司、坤御（北京）技术有限公司、金卡智能集团股份有限公司、江西捌零网络科技有限公司、江苏智运科技发展有限公司、江苏云湖现代服务产业集团有限公司、江苏敏捷科技股份有限公司、江苏麦维智能科技有限公司、嘉兴想天信息科技有限公司、济南索思信息技术有限公司、吉翁电子（深圳）有限公司、湖南建研信息技术股份有限公司、河南朝明教育科技有限公司、河北中翰合信税务师事务所有限公司、河北智旦网络科技有限公司、合肥图鸭信息科技有限公司、杭州知汇网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州麦途网络信息技术有限公司、杭州合泰软件有限公司、杭州海康威视数字技术股份有限公司、国交信息股份有限公司、广州图创计算机软件开发有限公司、广州同聚成电子科技有限公司、广州市奥威亚电子科技有限公司、广州九尾信息科技有限公司、广州泓颖网络科技有限公司、广联达科技股份有限公司、广东优信无限网络股份有限公司、广东优点云计算科技有限公司、广东飞企互联科技股份有限公司、佛山市杜特软件科技有限公司、泛微网络科技股份有限公司、鼎点视讯科技有限公司、帝国软件、郸城县新翔软件科技有限公司、大汉软件股份有限公司、成都智蜂网科技有限责任公司、成都星锐蓝海网络科技有限公司、郴州帝云网络科技有限公司、畅捷通信息技术股份有限公司、北京云因信息技术有限公司、北京友邻电子商务科技有限公司、北京亿赛通科技发展有限责任公司、北京信达网安科技有限公司、北京西骏数据科技股份有限公司、北京网康科技有限公司、北京网达立信信息技术有限公司、北京万户软件技术有限公司、北京通宇泰克科技股份有限公司、北京通达志成科技有限公司、北京通达信科科技有限公司、北京腾焰软件有限公司、北京搜狐互联网信息服务有限公司、北京神州视翰科技有限公司、北京猎鹰安全科技有限公司、北京雷速科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京金方时代科技有限公司、北京华清信安科技有限公司、北京宏景世纪软件股份有限公司、北京度友科技有限公司、北京东奥时代教育科技有限公司、北京大北农科技集团股份有限公司、北京超图软件股份有限公司、北京碧海威科技有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、安徽青柿信息科技有限公司、安徽七天网络科技有限公司、爱尔眼科医院集团、阿里巴巴集团安全应急响应中心、YXcms、XYCMS、LuckyFrameWeb、HadSky 和 classcms。

本周，CNVD 发布了《Microsoft 发布 2023 年 9 月安全更新》。详情参见 CNVD 网

站公告内容。

https://www.cnvd.org.cn/webinfo/show/9221

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、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、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等单位报送公开收集的漏洞数量较多。上海齐同信息科技有限公司、联想集团、快页信息技术有限公司、河南东方云盾信息技术有限公司、北京水木羽林科技有限公司、安徽锋刃信息科技有限公司、杭州美创科技有限公司、中电科网络安全科技股份有限公司、江苏云天网络安全技术有限公司、汇安云（山东）信息科技有限公司、河南悦海数安科技有限公司、上海谋乐网络科技有限公司、信息产业信息安全测评中心、苏州棱镜七彩信息科技有限公司、雅信科技、宁夏凯信特信息科技有限公司、深圳市魔方安全科技有限公司、广东盈世计算机科技有限公司、山东云天安全技术有限公司、北京众安天下科技有限公司、赛尔网络有限公司、西藏熙安信息技术有限责任公司、证通股份有限公司、国网湖北省电力有限公司恩施供电公司、中国电信股份有限公司上海研究院、北京远禾科技有限公司、河南灵创电子科技有限公司、南京聚铭网络科技有限公司、南方电网数字电网集团信息通信科技有限公司、安徽长泰科技有限公司、北京君云天下科技有限公司、北京机沃科技有限公司、博智安全科技股份有限公司、北京华耀科技有限公司、上海观安信息技术股份有限公司、北京中关村实验室、杭州飞致云信息科技有限公司、合肥梆梆信息科技有限公司、中孚安全技术有限公司、深圳昂楷科技有限公司、湖南中恒世纪科技有限公司、江苏极元信息技术有限公司、超聚变数字技术有限公司、亚信科技（成都）有限公司及其他个人白帽子向 CNVD 提交了 8319 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）、上海交和三六零数字安全科技集团有限公司和向 CNVD 共享的白帽子报送的 5864 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）	4020	4020
奇安信网神（补天平台）	1064	1064
北京神州绿盟科技有限公司	833	3
北京启明星辰信息安全技术有限公司	531	13

新华三技术有限公司	524	0
上海交大	462	462
三六零数字安全科技集团有限公司	318	318
安天科技集团股份有限公司	280	0
北京天融信网络安全技术有限公司	209	0
深信服科技股份有限公司	163	1
北京数字观星科技有限公司	160	0
中国电信股份有限公司网络安全产品运营中心	131	131
阿里云计算有限公司	112	13
北京长亭科技有限公司	91	7
天津市国瑞数码安全系统股份有限公司	55	0
北京知道创宇信息技术有限公司	53	0
远江盛邦（北京）网络安全科技股份有限公司	36	36
杭州迪普科技股份有限公司	20	0
南京联成科技发展股份有限公司	12	12
浙江大华技术股份有限公司	10	10
深圳市腾讯计算机系统有限公司（玄武实验室）	3	3
杭州安恒信息技术股	3	3

份有限公司		
北京智游网安科技有限公司	2	2
西安四叶草信息技术有限公司	1	1
京东科技信息技术有限公司	1	1
上海齐同信息科技有限公司	161	161
联想集团	125	125
快页信息技术有限公司	39	39
河南东方云盾信息技术有限公司	38	38
北京水木羽林科技有限公司	35	35
亚信科技（成都）有限公司	34	34
安徽锋刃信息科技有限公司	31	31
西门子（中国）有限公司	23	0
杭州美创科技有限公司	18	18
中电科网络安全科技股份有限公司	10	10
江苏云天网络安全技术有限公司	10	10
汇安云（山东）信息科技有限公司	9	9
河南悦海数安科技有限公司	7	7
上海谋乐网络科技有限公司	7	7
信息产业信息安全测	5	5

评中心		
苏州棱镜七彩信息科技有限公司	4	4
雅信科技	3	3
宁夏凯信特信息科技有限公司	3	3
深圳市魔方安全科技有限公司	3	3
广东盈世计算机科技有限公司	3	3
山东云天安全技术有限公司	3	3
北京众安天下科技有限公司	2	2
赛尔网络有限公司	2	2
西藏熙安信息技术有限责任公司	2	2
证通股份有限公司	2	2
国网湖北省电力有限公司恩施供电公司	2	2
中国电信股份有限公司上海研究院	2	2
北京远禾科技有限公司	2	2
河南灵创电子科技有限公司	2	2
南京聚铭网络科技有限公司	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
安徽长泰科技有限公司	1	1
北京君云天下科技有限公司	1	1

北京机沃科技有限公司	1	1
博智安全科技股份有限公司	1	1
北京华耀科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
北京中关村实验室	1	1
杭州飞致云信息科技有限公司	1	1
合肥梆梆信息科技有限公司	1	1
中孚安全技术有限公司	1	1
深圳昂楷科技有限公司	1	1
湖南中恒世纪科技有限公司	1	1
江苏极元信息技术有限公司	1	1
超聚变数字技术有限公司	1	1
个人	1639	1639
报送总计	11336	8319

本周漏洞按类型和厂商统计

本周，CNVD 收录了 437 个漏洞。WEB 应用 191 个，应用程序 124 个，网络设备（交换机、路由器等网络端设备）88 个，智能设备（物联网终端设备）12 个，操作系统 11 个，安全产品 10 个，区块链外围系统 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	191
应用程序	124
网络设备（交换机、路由器等网络端设备）	88

智能设备（物联网终端设备）	12
操作系统	11
安全产品	10
区块链外围系统	1

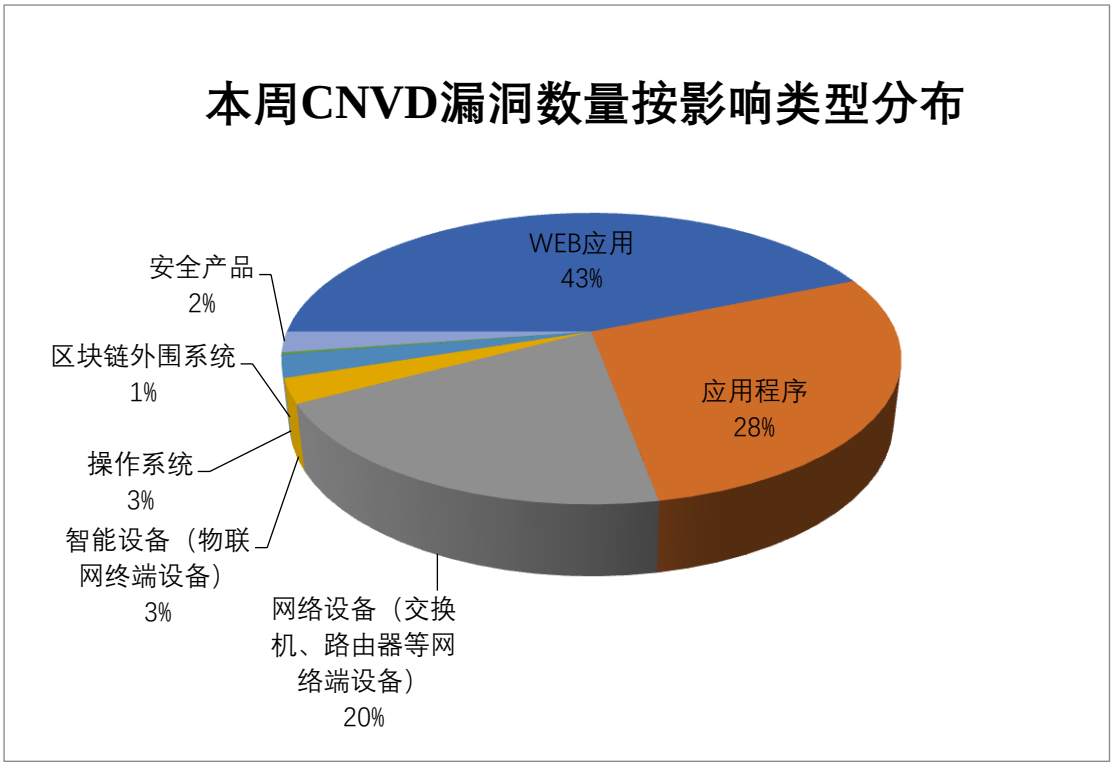

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Siemens、H3C 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	28	7%
2	Siemens	14	3%
3	H3C	14	3%
4	Google	12	3%
5	IBM	12	3%
6	北京百卓网络技术有限公司	11	2%
7	Mozilla	11	2%
8	Tenda	8	2%
9	杭州雄伟科技开发股份有限公司	8	2%
10	其他	319	73%

本周行业漏洞收录情况

本周，CNVD 收录了 57 个电信行业漏洞，57 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2023-69035）、Siemens SIMATIC 产品 ANSI C OPC UA SDK 拒绝服务漏洞”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/

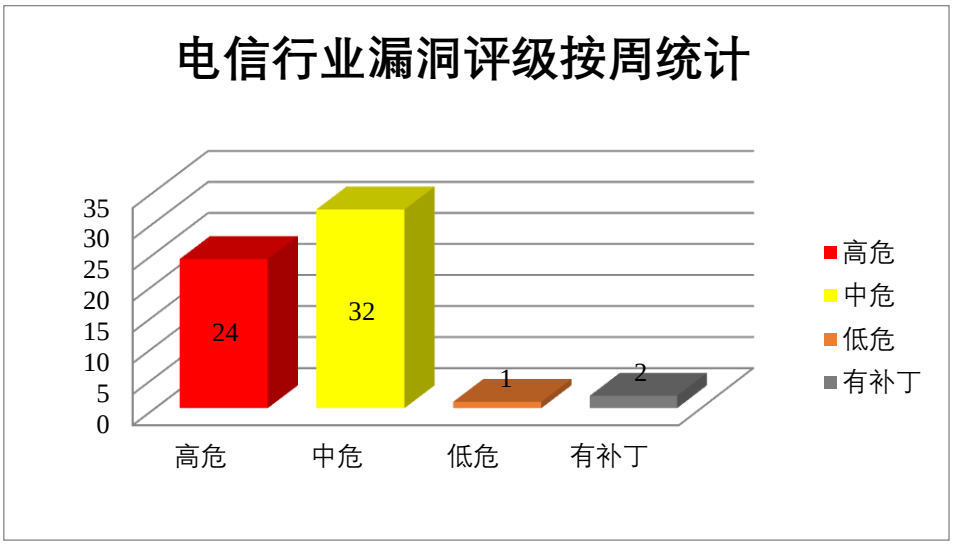

图 3 电信行业漏洞统计

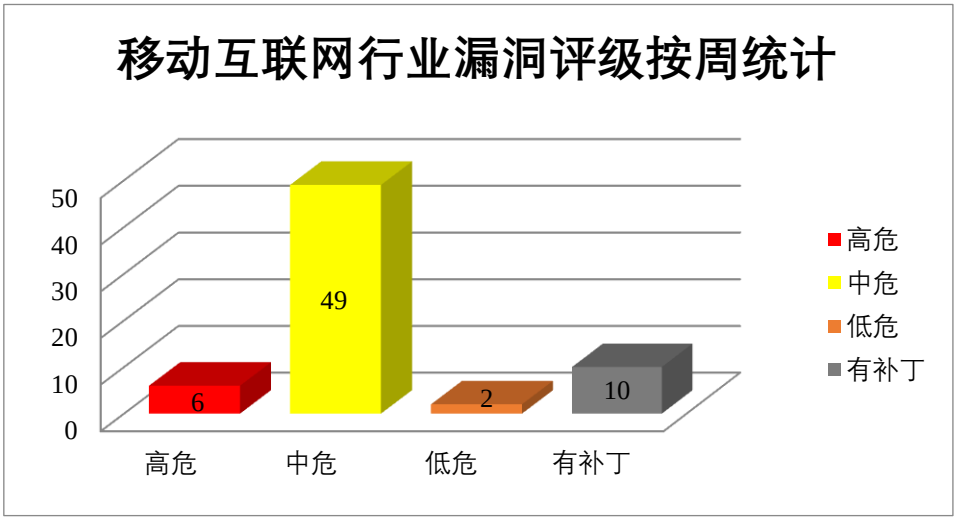

图 4 移动互联网行业漏洞统计

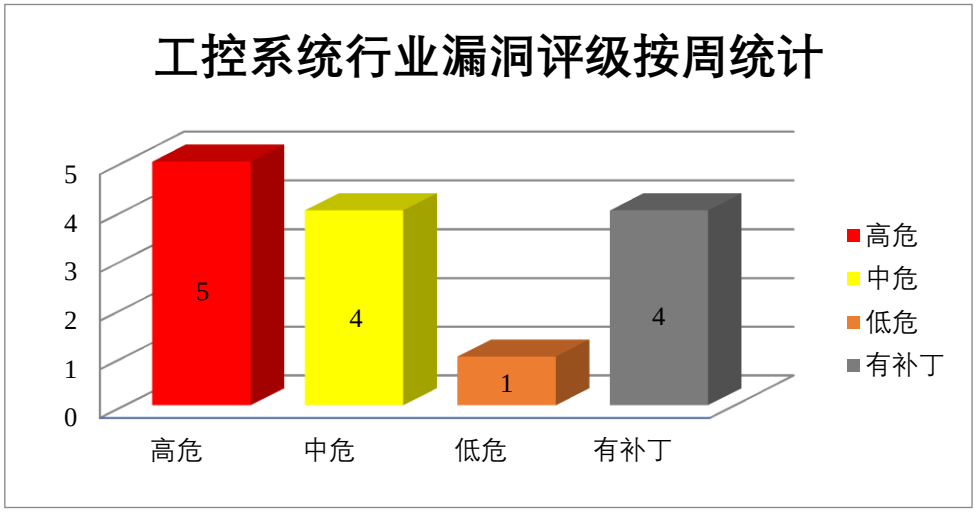

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Android 是美国谷歌(Google)公司的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，造成拒绝服务，在系统上获得提升的权限。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-69035、CNVD-2023-69042、CNVD-2023-69045、CNVD-2023-69046）、Google Android 信息泄露漏洞（CNVD-2023-69040、CNVD-2023-69041、CNVD-2023-69044）、Google Android 拒绝服务漏洞（CNVD-2023-69043）。其中，“Google Android 权限提升漏洞（CNVD-2023-69035、CNVD-2023-69042、CNVD-2023-69045、CNVD-2023-69046）”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-2023-69035

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69040

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69041

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69042

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69043

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69044

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69045

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69046

2、 Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。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网络安全检查，获取敏感信息，在系统上执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2023-68439、CNVD-2023-68481）、Mozilla Firefox 代码执行漏洞（CNVD-2023-68438、CNVD-2023-68441、CNVD-2023-68478）、Mozilla Firefox 拒绝服务漏洞（CNVD-2023-68440）、Mozilla Firefox 安全绕过漏洞（CNVD-2023-68482、CNVD-2023-68480）。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-2023-68439

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68438

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68441

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68440

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68478

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68482

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68481

https://www.cnvd.org.cn/flaw/show/CNVD-2023-68480

3、IBM 产品安全漏洞

IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。IBM Security Verify Access（ISAM）是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM Sterling Connect:Direct 是美国国际商业机器（IBM）公司的一套基于文件的点对点文件传输解决方案。IBM TXSeries for Multiplatforms 是美国国际商业机器（IBM）公司的一种事务处理监控和管理的软件产品，它旨在支持多平台上的分布式事务处理。IBM Robotic Process Automation 是美国国际商业机器（IBM）公司的一种机器人流程自动化产品。可帮助您以传统 RPA 的轻松和速度大规模自动化更多业务和 IT 流程。IBM Security Guardium 是美国国际商业机器（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 Planning Analytics 是美国国际商业机器（IBM）公司的一套业务规划分析解决方案。该方案支持自动化执行业务规划、预算和分析等流程。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞使用开放重定向进行网络钓鱼攻击，访问敏感文件，提升权限，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2023-68779）、IBM Security Verify Access 输入验证错误漏洞（CNVD-2023-687

78）、IBM Sterling Connect:Direct 加密问题漏洞、IBM TXSeries for Multiplatforms 拒绝服务漏洞、IBM Robotic Process Automation 授权问题漏洞（CNVD-2023-68780）、IBM Security Guardium 授权问题漏洞（CNVD-2023-68784）、IBM Planning Analytics 加密问题漏洞（CNVD-2023-68783）、IBM Security Guardium 输入验证错误漏洞。其中，“IBM Sterling Connect:Direct 加密问题漏洞、IBM TXSeries for Multiplatforms 拒绝服务漏洞”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-2023-68779
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68778
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68777
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68776
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68780
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68784
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68783
https://www.cnvd.org.cn/flaw/show/CNVD-2023-68785

4、Siemens 产品安全漏洞

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。Siemens Parasolid 是一种三维几何建模工具，支持各种技术，包括实体建模、直接编辑和自由曲面/图纸建模。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。

CNVD 收录的相关漏洞包括：Siemens Teamcenter Visualization 和 JT2Go 堆栈缓冲区溢出漏洞（CNVD-2023-69804、CNVD-2023-69810）、Siemens Teamcenter Visualization 和 JT2Go 类型混淆漏洞、Siemens Teamcenter Visualization 和 JT2Go 内存错误引用漏洞（CNVD-2023-69805）、Siemens Teamcenter Visualization 和 JT2Go 类型混淆漏洞（CNVD-2023-69807）、Siemens Teamcenter Visualization 和 JT2Go 堆缓冲区溢出漏洞（CNVD-2023-69809）、Siemens Teamcenter Visualization 和 JT2Go 越界写入漏洞（CNVD-2023-69808）、Siemens Parasolid 越界写入漏洞（CNVD-2023-69813）。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-2023-69804
https://www.cnvd.org.cn/flaw/show/CNVD-2023-69806
https://www.cnvd.org.cn/flaw/show/CNVD-2023-69805
https://www.cnvd.org.cn/flaw/show/CNVD-2023-69807
https://www.cnvd.org.cn/flaw/show/CNVD-2023-69809
https://www.cnvd.org.cn/flaw/show/CNVD-2023-69808

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69810

https://www.cnvd.org.cn/flaw/show/CNVD-2023-69813

5、Tenda AC23 sub_451784 函数堆栈溢出漏洞

Tenda AC23 是中国腾达（Tenda）公司的一款双频千兆无线路由器。本周，Tenda AC23 被披露存在堆栈溢出漏洞。该漏洞源于 sub_451784 函数未能正确验证输入数据的长度大小，攻击者可利用该漏洞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-2023-69722

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-2023-68438	Mozilla Firefox 代码执行漏洞（CNVD-2023-68438）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/
CNVD-2023-68442	Mozilla Firefox for iOS 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2023-25/
CNVD-2023-68481	Mozilla Firefox 信息泄露漏洞（CNVD-2023-68481）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2023-01/
CNVD-2023-68479	Mozilla Firefox 信息泄露漏洞（CNVD-2023-68479）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/security/advisories/mfsa2023-22/
CNVD-2023-68776	IBM TXSeries for Multiplatforms 拒绝服务漏洞	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/7025476
CNVD-2023-69036	Google Chrome MediaStream 内存错误引用漏洞（CNVD-2023-69036）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_29.html
CNVD-2023-69045	Google Android 权限提升漏洞（CNVD-2023-69045）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/b

			ulletin/2023-08-01
CNVD-2023-69803	Siemens SIMATIC 产品 ANSI C OPC UA SDK 拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-711309.html
CNVD-2023-69811	Siemens Industrial 产品 WIBU 系统 CodeMeter 堆缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-240541.html
CNVD-2023-69812	Siemens Parasolid 越界写入漏洞（CNVD-2023-69812）	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-190839.html

小结：本周，Google 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，造成拒绝服务，在系统上获得提升的权限。此外，Mozilla、IBM、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过网络安全检查，使用开放重定向进行网络钓鱼攻击，访问敏感文件，提升权限，在系统上执行任意代码或导致拒绝服务等。另外，Tenda AC23 被披露存在堆栈溢出漏洞。攻击者可利用该漏洞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、Simple Cold Storage Management System SQL 注入漏洞（CNVD-2023-69723）

验证描述

Simple Cold Storage Management System 是一个简易冷库管理系统。

Simple Cold Storage Management System 存在 SQL 注入漏洞。攻击者可利用该漏洞查看、添加、修改或删除后端数据库中的信息。

验证信息

POC 链接：http://packetstormsecurity.com/files/169605/Simple-Cold-Storage-Management-System-1.0-SQL-Injection.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-69723

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. Mozilla 紧急修补 Firefox 和 Thunderbird 中的 WebP 零日漏洞

Mozilla 周二发布了安全更新，修复了 Firefox 和 Thunderbird 中的零日漏洞。该漏洞被标记为 CVE-2023-4863，是 WebP 图像格式中的堆缓冲区溢出漏洞，在处理特制图像时可能导致任意代码执行。

参考链接：https://thehackernews.com/2023/09/mozilla-rushes-to-patch-webp-critical.html

2. GitHub 曝出漏洞，或导致多个存储库遭受劫持攻击

安全研究员发现 GitHub 中存在一个新安全漏洞，该漏洞可能导致数千个存储库面临劫持攻击的风险。

参考链接：https://thehackernews.com/2023/09/critical-github-vulnerability-exposes.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