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 25 日-2023 年 10 月 08 日 **2023 年第 39、40 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 562 个，其中高危漏洞 198 个、中危漏洞 296 个、低危漏洞 68 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 356 个（占 63%），其中互联网上出现“WBCE CMS 任意文件上传漏洞（CNVD-2023-71724）、Boom CMS 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 10321 个，与上周（17693 个）环比减少 42%。

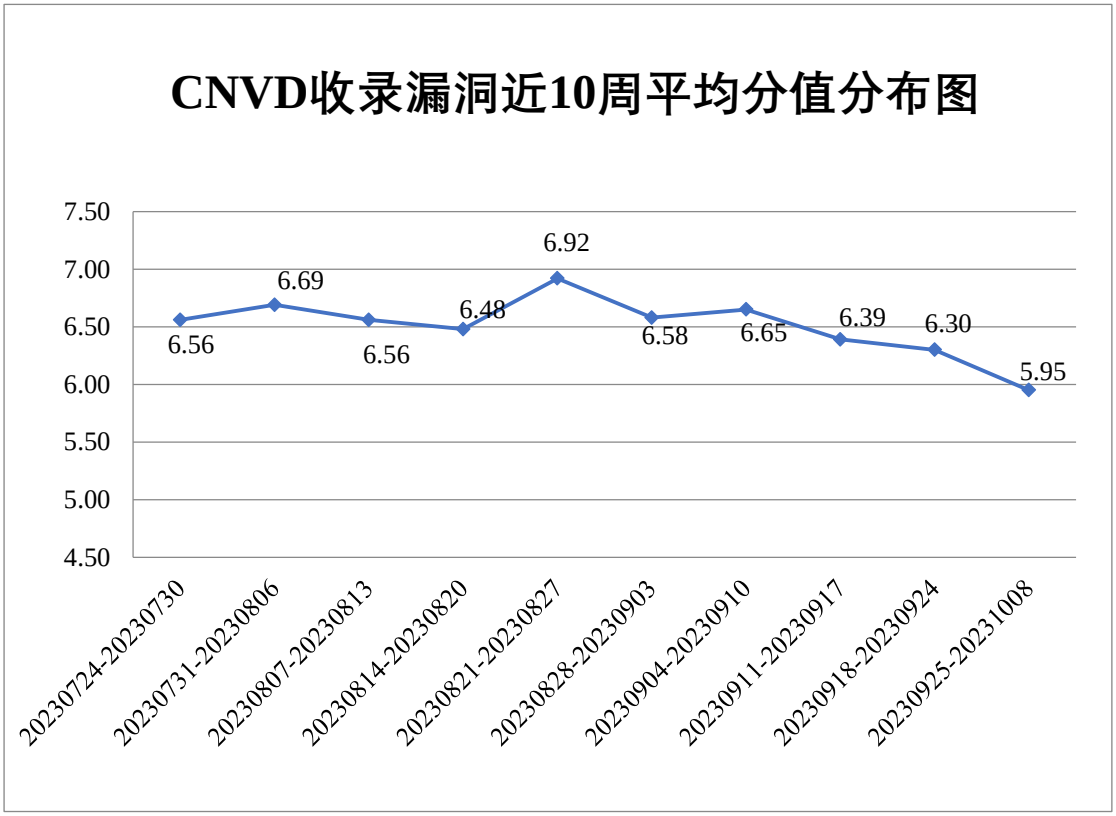

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 39 起，向基础电信企业通报漏洞事件 16 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 1041 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 149 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 89 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：

佐藤控股股份有限公司、紫光软件系统有限公司、淄博闪灵网络科技有限公司、珠海优特电力科技股份有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、重庆耐德工业股份有限公司、众勤通信设备贸易（上海）有限公司、中控技术股份有限公司、中科方德软件有限公司、中海创科技（福建）集团有限公司、浙江宇视科技有限公司、浙江火文科技有限公司、浙江大华技术股份有限公司、圆动（上海）信息技术服务有限公司、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、阳光电源股份有限公司、徐州小跃跃跑腿服务有限公司、兄弟（中国）商业有限公司、星软集团有限公司、西安众邦网络科技有限公司、西安网络盾网络技术有限公司、武汉职多多网络科技有限公司、武汉天际航信息科技股份有限公司、温州互引信息技术有限公司、威海市天罡仪表股份有限公司、通州区华丽软件工作室、天津天堰科技股份有限公司、天宝莅德电子科技（上海）有限公司北京分公司、太仓市浮桥镇盛中房产中介、宿迁乐视传媒有限公司、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、四创科技有限公司、四川曾龙海奢荟实业有限公司、首码信息技术（北京）有限公司、世邦通信股份有限公司、石家庄友曼网络科技有限公司、昇频股份有限公司、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、深圳市中兴新云服务有限公司、深圳市易宇通科技有限公司、深圳市雄帝科技股份有限公司、深圳市微控一指通科技有限公司、深圳市网域科技股份有限公司、深圳市通邮物流科技（集团）股份有限公司、深圳市联新移动医疗科技有限公司、深圳市东方博雅科技有限公司、深圳市道通智能航空技术股份有限公司、申瓯通信设备有限公司、绍兴易新网络技术服务有限公司、上海卓卓网络科技有限公司、上海迅饶自动化科技有限公司、上海熙软科技有限公司、上海淘满家电子商务有限公司、上海企源科技股份有限公司、上海肯特仪表股份有限公司、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、上海博达数据通信有限公司、上海宝信软件股份有限公司、熵基科技股份有限公司、陕西星枫科技有限公司、山西生活向导网络科技有限公司、山西青峰软件股份有限公司、山石网科通信技术股份有限公司、山脉科技股份有限公司、山东中维世纪科技股份有限公司、山东运筹软件有限公司、

山东光辉人力资源科技有限公司、山东锋士信息技术有限公司、厦门一指通智能科技有限公司、厦门眼科中心有限公司、厦门康强人才服务有限公司、三七信息产业有限公司、睿云联（厦门）网络通讯技术有限公司、融智通科技（北京）股份有限公司、青峰软件有限公司、青岛惊喜优品科技有限公司、青岛海信网络科技股份有限公司、青岛东软载波科技股份有限公司、麒麟软件有限公司、普联技术有限公司、鹏为软件股份有限公司、欧普康视科技股份有限公司、迈普通信技术股份有限公司、罗格朗（上海）管理有限公司、柳州新云网络科技有限公司、联众智慧科技股份有限公司、联奕科技股份有限公司、乐清市运输集团有限公司、科大讯飞股份有限公司、焦作市讯腾网络技术有限公司、江西汇满鑫科技有限公司、江苏赛达电子科技有限公司、济宁云课网络科技有限公司、吉翁电子（深圳）有限公司、慧景科技有限公司、慧聪云商（佛山）网络科技有限公司、淮南市银泰软件科技有限公司、湖南思博特信息科技有限公司、河南信合建设投资集团有限公司、河南航天金穗电子有限公司、河北一六八网络科技有限公司、杭州言商网络技术有限公司、杭州叙简科技股份有限公司、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、杭州蓝代斯克数字技术有限公司、杭州海康威视数字技术股份有限公司、杭州边锋网络技术有限公司、广州图创计算机软件开发有限公司、广州市天翎网络科技有限公司、广州达梦网络科技有限公司、广东鑫宝软件科技有限公司、广东伟达智能装备股份有限公司、广东世纪信通科技股份有限公司、广东省燕巢网络科技有限公司、广东健康在线信息技术股份有限公司、广东建安信息科技有限公司、广东广大信息技术科技有限公司、彩讯科技股份有限公司、甘肃中联人力资源有限公司、富士胶片商业创新（中国）有限公司、福州慧美丰科技有限公司、福建易洁科技有限公司、福建亿能达信息技术股份有限公司、福建省四信数字科技集团有限公司、福建省海峡信息技术有限公司、福建泉州匹克体育用品有限公司、福建盟购信息科技有限公司、福建八方好帮手人力资源服务有限公司、佛山市东汇网络技术有限公司、东方希望集团有限公司、成都市智蜂网科技有限责任公司、成都零起飞科技有限公司、成都江鼎禹丰科技有限公司、畅捷通信息技术股份有限公司、北汽福田汽车股份有限公司、北京中远麒麟科技有限公司、北京中创视讯科技有限公司、北京智邦国际软件技术有限公司、北京赢才科技有限公司、北京阳光第一车网科技有限公司、北京选优科技有限公司、北京文华在线教育科技股份有限公司、北京微梦创科网络技术有限公司、北京网康科技有限公司、北京万维盈创科技发展有限公司、北京胜能能源科技有限公司、北京睿智博创科技有限公司、北京美特软件技术有限公司、北京蓝色创想网络科技有限责任公司、北京开心人信息技术有限公司、北京金和网络股份有限公司、北京基调网络股份有限公司、北京火木科技有限公司、北京华宇信息技术有限公司、北京宏景世纪软件股份有限公司、北京国通创安报警网络技术有限公司、北京百卓网络技术有限公司、北京安普诺信息技术有限公司、宝宝巴士（福建）网络科技有限公司、巴中人才网人力资源有限公司、奥琦玮信息科技（北京）有限公司、傲拓科技股份有限公司、安徽中科智泰光电测控科技有

限公司、安徽中技国医医疗科技有限公司、安徽南瑞继远电网技术有限公司和 SEMCMS。

本周，CNVD 发布了《关于 libwebp 开源库存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9331

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、安天科技集团股份有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。亚信科技（成都）有限公司、博智安全科技股份有限公司、联想集团、安徽锋刃信息科技有限公司、快页信息技术有限公司、河南东方云盾信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、杭州默安科技有限公司、河南灵创电子科技有限公司、内蒙古洞明科技有限公司、西藏熙安信息技术有限责任公司、中孚安全技术有限公司、中国电信股份有限公司上海研究院、汇安云（山东）信息科技有限公司、工业和信息化部电子第五研究所-数据治理服务中心、河南信安世纪科技有限公司、深圳市魔方安全科技有限公司、赛尔网络有限公司、成都卓越华安信息技术服务有限公司、北京山石网科信息技术有限公司、湖南泛联新安信息科技有限公司、江苏天竞云合数据技术有限公司、山东云天安全技术有限公司、上海直画科技有限公司、广东粤密技术服务有限公司、河南悦海数安科技有限公司、上海纽盾科技股份有限公司、中电智安科技有限公司、北京天防安全科技有限公司、信息产业信息安全测评中心、北京众安天下科技有限公司、北京网御星云信息技术有限公司、南京聚铭网络科技有限公司、合肥梆梆信息科技有限公司、山东正中信息技术股份有限公司、山东新潮信息技术有限公司、南京深安科技有限公司、浙江中控技术股份有限公司、苏州棱镜七彩信息科技有限公司、星云博创科技有限公司、中国工商银行、江苏金陵科技集团有限公司、成都安美勤信息技术股份有限公司、统信软件技术有限公司、北京君云天下科技有限公司、建信金科网络攻击实验室、广州安亿信软件科技有限公司、北京中关村实验室、深圳昂楷科技有限公司、江苏晟晖信息科技有限公司及其他个人白帽子向 CNVD 提交了 10321 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 7368 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）	3179	3179
斗象科技（漏洞盒子）	2097	2097

上海交大	1596	1596
北京启明星辰信息安全技术有限公司	1007	5
北京天融信网络安全技术有限公司	596	3
新华三技术有限公司	530	0
三六零数字安全科技集团有限公司	496	496
安天科技集团股份有限公司	352	1
阿里云计算有限公司	223	0
北京数字观星科技有限公司	175	0
杭州安恒信息技术股份有限公司	100	6
北京神州绿盟科技有限公司	88	0
北京长亭科技有限公司	69	0
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	51	0
中国电信集团系统集成有限责任公司	27	0
杭州迪普科技股份有限公司	20	0
中电科网络安全科技股份有限公司	16	16
南京联成科技发展股份有限公司	9	9
北京智游网安科技有限公司	5	5
远江盛邦（北京）网络安全科技股份有限	3	3

公司		
浙江大华技术股份有限公司	2	2
中国电信股份有限公司网络安全产品运营中心	1	1
恒安嘉新（北京）科技股份公司	1	0
贵州泰若数字科技有限公司	1	1
亚信科技（成都）有限公司	634	634
博智安全科技股份有限公司	291	291
联想集团	109	109
安徽锋刃信息科技有限公司	38	38
快页信息技术有限公司	34	34
河南东方云盾信息技术有限公司	31	31
奇安星城网络安全运营服务（长沙）有限公司	19	19
杭州默安科技有限公司	10	10
河南灵创电子科技有限公司	9	9
内蒙古洞明科技有限公司	9	9
西藏熙安信息技术有限责任公司	7	7
中孚安全技术有限公司	6	6
中国电信股份有限公	5	5

司上海研究院		
汇安云（山东）信息科技有限公司	5	5
工业和信息化部电子第五研究所-数据治理服务中心	5	5
河南信安世纪科技有限公司	4	4
深圳市魔方安全科技有限公司	4	4
赛尔网络有限公司	3	3
成都卓越华安信息技术服务有限公司	3	3
北京山石网科信息技术有限公司	3	3
湖南泛联新安信息科技有限公司	3	3
江苏天竞云合数据技术有限公司	3	3
山东云天安全技术有限公司	2	2
上海直画科技有限公司	2	2
广东粤密技术服务有限公司	2	2
河南悦海数安科技有限公司	2	2
上海纽盾科技股份有限公司	2	2
中电智安科技有限公司	2	2
北京天防安全科技有限公司	2	2
信息产业信息安全测评中心	2	2

北京众安天下科技有限公司	2	2
北京网御星云信息技术有限公司	2	2
南京聚铭网络科技有限公司	2	2
合肥梆梆信息科技有限公司	1	1
山东正中信息技术股份有限公司	1	1
山东新潮信息技术有限公司	1	1
南京深安科技有限公司	1	1
浙江中控技术股份有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
星云博创科技有限公司	1	1
中国工商银行	1	1
江苏金陵科技集团有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
统信软件技术有限公司	1	1
北京君云天下科技有限公司	1	1
建信金科网络攻击实验室	1	1
广州安亿信软件科技有限公司	1	1
北京中关村实验室	1	1
深圳昂楷科技有限公	1	1

司		
江苏晟晖信息科技有限公司	1	1
CNCERT 广西分中心	8	8
CNCERT 贵州分中心	6	6
CNCERT 河北分中心	5	5
CNCERT 内蒙古分中心	1	1
CNCERT 陕西分中心	1	1
个人	1606	1606
报送总计	13604	10321

本周漏洞按类型和厂商统计

本周，CNVD 收录了 562 个漏洞。WEB 应用 234 个，应用程序 179 个，网络设备（交换机、路由器等网络端设备）69 个，智能设备（物联网终端设备）44 个，操作系统 18 个，安全产品 15 个，数据库 2 个，车联网 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	234
应用程序	179
网络设备（交换机、路由器等网络端设备）	69
智能设备（物联网终端设备）	44
操作系统	18
安全产品	15
数据库	2
车联网	1

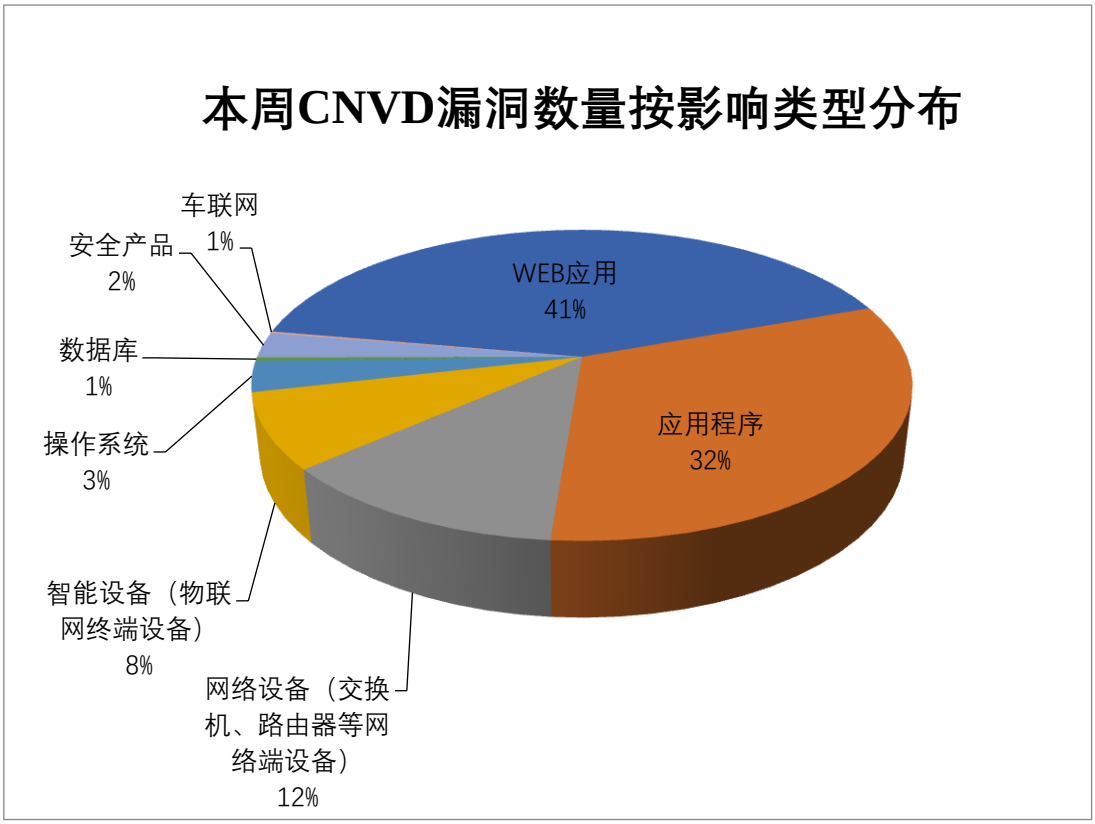

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Samsung、Microsoft 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	WordPress	26	5%
2	Samsung	23	4%
3	Microsoft	21	4%
4	Adobe	19	3%
5	Apache	13	2%
6	Linux	10	2%
7	北京网康科技有限公司	8	2%
8	Oracle	7	1%
9	上海泛微网络科技股份有限公司	7	1%
10	其他	428	76%

本周行业漏洞收录情况

本周，CNVD 收录了 46 个电信行业漏洞，86 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“ASUS RT-AX82U 拒绝服务漏洞、Samsung Settings

输入验证错误漏洞（CNVD-2023-73907）”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/

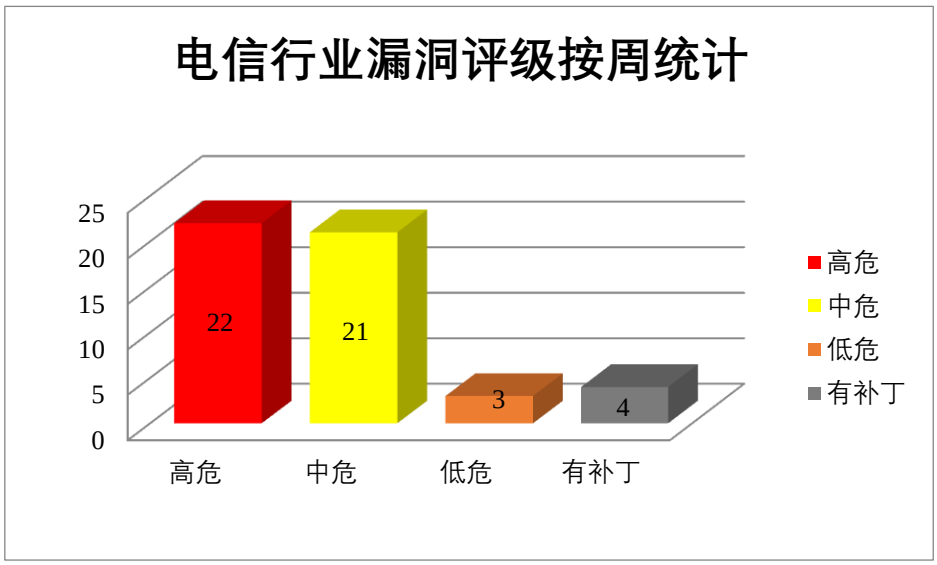

图 3 电信行业漏洞统计

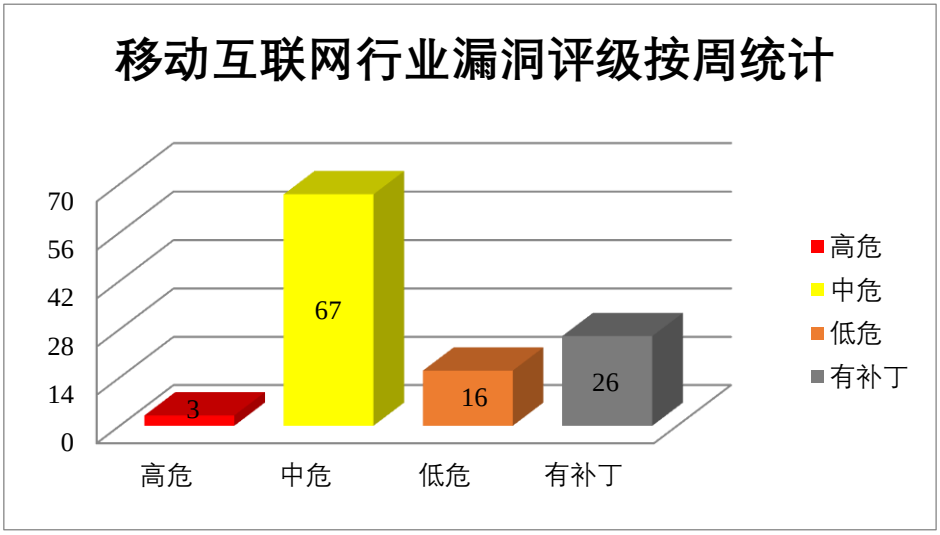

图 4 移动互联网行业漏洞统计

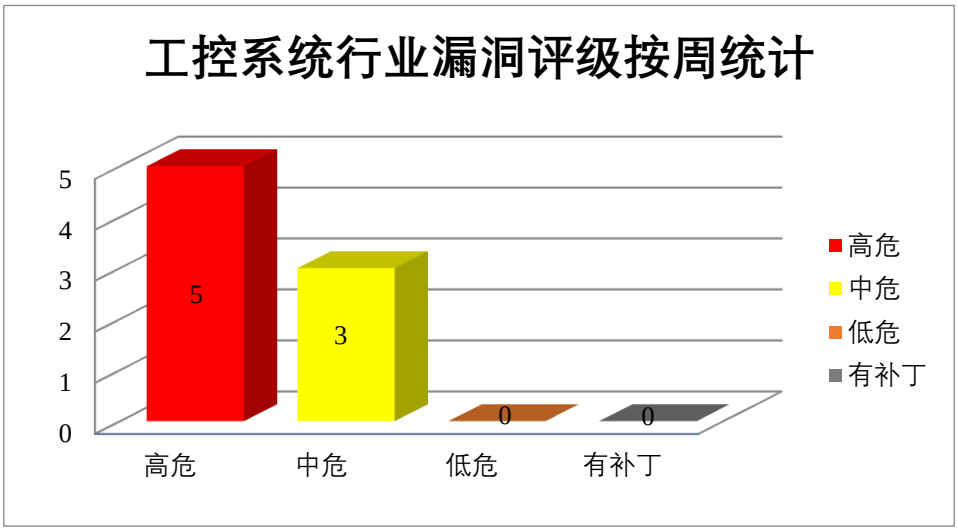

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2023-72202）、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2023-72224、CNVD-2023-72225、CNVD-2023-72227、CNVD-2023-72228）、Microsoft Exchange Server 欺骗漏洞（CNVD-2023-72226、CNVD-2023-72230、CNVD-2023-72231）。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-2023-72202

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72224

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72225

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72226

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72227

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72228

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72230

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72231

2、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越界读取，使系统崩溃或提升他们在系统上的权限等。

CNVD 收录的相关漏洞包括：Linux Kernel 拒绝服务漏洞（CNVD-2023-71723）、Linux kernel 内存错误引用漏洞（CNVD-2023-71722）、Linux kernel 条件竞争漏洞（CNVD-2023-71721）、Linux kernel smb2misc.c 文件越界读取漏洞、Linux kernel connection.c 文件越界读取漏洞、Linux kernel Ext4 文件系统内存错误引用漏洞、Linux kernel 内存错误引用漏洞（CNVD-2023-72243）、Linux Kernel eBPF 本地权限提升漏洞。其中，“Linux kernel smb2misc.c 文件越界读取漏洞、Linux kernel connection.c 文件越界读取漏洞、Linux kernel 内存错误引用漏洞（CNVD-2023-72243）”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-2023-71723
https://www.cnvd.org.cn/flaw/show/CNVD-2023-71722
https://www.cnvd.org.cn/flaw/show/CNVD-2023-71721
https://www.cnvd.org.cn/flaw/show/CNVD-2023-72241
https://www.cnvd.org.cn/flaw/show/CNVD-2023-72240
https://www.cnvd.org.cn/flaw/show/CNVD-2023-72244
https://www.cnvd.org.cn/flaw/show/CNVD-2023-72243
https://www.cnvd.org.cn/flaw/show/CNVD-2023-74539

3、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。Adobe Illustrator 是美国奥多比（Adobe）公司的一套基于向量的图像制作软件。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 NTLMv2 凭据，导致应用程序拒绝服务，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2023-71744）、Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2023-71750、CNVD-2023-71749）、Adobe Acrobat Reader 释放后重用漏洞（CNVD-2023-71752、CNVD-2023-71754、CNVD-2023-71756、CNVD-2023-71759）、Adobe Illustrator 越界写入漏洞（CNVD-2023-74542）。其中，除“Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2023-71750）、Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2023-71749）”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-2023-71744
https://www.cnvd.org.cn/flaw/show/CNVD-2023-71750
https://www.cnvd.org.cn/flaw/show/CNVD-2023-71749

https://www.cnvd.org.cn/flaw/show/CNVD-2023-71752

https://www.cnvd.org.cn/flaw/show/CNVD-2023-71754

https://www.cnvd.org.cn/flaw/show/CNVD-2023-71756

https://www.cnvd.org.cn/flaw/show/CNVD-2023-71759

https://www.cnvd.org.cn/flaw/show/CNVD-2023-74542

4、Apache 产品安全漏洞

Apache Traffic Server（ATS）是美国阿帕奇（Apache）基金会的一套可扩展的 HTTP 代理和缓存服务器。Apache MINA 是美国阿帕奇（Apache）基金会的一款网络应用程序框架。该产品主要用于开发高性能和高可伸缩性的网络应用程序。Apache OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache Flink 是美国 Apache 基金会的一款开源的分布式流数据处理引擎。该产品主要使用 Java 和 Scala 语言编写。Func 是 Knative 开源的一个客户端库和 CLI ，支持功能的开发和部署。Apache Airflow 是美国阿帕奇（Apache）基金会的一套用于创建、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 Superset 是美国阿帕奇（Apache）基金会的一个数据可视化和数据探索平台。Apache DolphinScheduler 是美国阿帕奇（Apache）基金会的一个分布式的基于 DAG 可视化的工作流任务调度系统。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，注入恶意内容到发送到用户浏览器的 HTTP 响应中，导致服务端请求伪造攻击等。

CNVD 收录的相关漏洞包括：Apache Traffic Server 信息泄露漏洞（CNVD-2023-71727）、Apache MINA 信息泄露漏洞、Apache OFBiz 路径遍历漏洞、Apache Flink 代码注入漏洞、Apache Airflow 授权问题漏洞（CNVD-2023-72233）、Apache Superset 授权问题漏洞、Apache Superset REST API 授权问题漏洞、Apache DolphinScheduler 授权问题漏洞。其中，“Apache Traffic Server 信息泄露漏洞（CNVD-2023-71727）、Apache OFBiz 路径遍历漏洞”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-2023-71727

https://www.cnvd.org.cn/flaw/show/CNVD-2023-71726

https://www.cnvd.org.cn/flaw/show/CNVD-2023-71730

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72234

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72233

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72237

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72236

https://www.cnvd.org.cn/flaw/show/CNVD-2023-72239

5、Zoo Management System SQL 注入漏洞（ CNVD-2023-72245）

Zoo Management System 是一个动物园管理系统。为动物园企业提供了一个在线和自动化平台来管理他们的日常记录。本周，Zoo Management System 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。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-2023-72245

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-2023-74532	NXLog Manager 存在跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://nxlog.co
CNVD-2023-74535	emlog pro /admin/plugin.php 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/emlog/
CNVD-2023-74537	mojoPortal 存在文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mojoportal.com/
CNVD-2023-74542	Adobe Illustrator 越界写入漏洞（CNVD-2023-74542）	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/illustrator/apsb22-26.html
CNVD-2023-71744	Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2023-71744）	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/apsb19-55.html
CNVD-2023-72246	answer 访问控制错误漏洞（CNVD-2023-72246）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/answerdev/answer/commit/e75142a55546e01d8904f59db228422561f51666
CNVD-2023-72247	CuppaCMS 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/CuppaCMS/CuppaCMS
CNVD-2023-72249	Vim 缓冲区溢出漏洞（CNVD-2023-72249）	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://github.com/vim/vim/commit/f6d28fe2c95c678cc3202cc5dc825a3fcc709e93

CNVD-2023-72254	Wireshark 拒绝服务漏洞（CNVD-2023-72254）	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://www.wireshark.org/security/wnpa-sec-2023-24.html
CNVD-2023-72258	ASUS RT-AX82U 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://www.asus.com/us/networking-iot-servers/wifi-routers/asus-gaming-routers/rt-ax82u/

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，在系统上执行任意代码等。此外，Linux、Adobe、Apache 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，注入恶意内容到发送到用户浏览器的 HTTP 响应中，导致服务端请求伪造攻击，导致越界读取，使系统崩溃或提升他们在系统上的权限等。另外，Zoo Management System 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。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、WBCE CMS 任意文件上传漏洞（CNVD-2023-71724）

验证描述

WBCE CMS 是一套基于 PHP 和 MySQL 的开源内容管理系统（CMS）。

WBCE CMS 1.6.1 版本存在任意文件上传漏洞，该漏洞源于/languages/install.php 组件中对上传的文件缺少有效的验证。攻击者可利用该漏洞上传恶意文件从而远程执行任意代码。

验证信息

POC 链接：https://gitee.com/CTF-hacker/pwn/issues/I7LH2N

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-71724

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. 超微 BMC 固件曝 7 个高危漏洞

超微（Supermicro）底板管理控制器（BMC）的智能平台管理接口（IPMI）固件中存在多个安全漏洞，这些漏洞可能导致权限升级，并在受影响的系统上执行恶意代码。

参考链接：https://thehackernews.com/2023/10/supermicros-bmc-firmware-found.html

2. 谷歌将于 2024 年加强网络钓鱼和恶意软件传递防御

Google 将从 2024 年起为电子邮件发件人引入新的指南，以便加强安全 Gmail 电子邮件并防止网络钓鱼诈骗和恶意软件传递。

参考链接：http://www.anquan419.com/knews/24/5931.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