国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 10 月 16 日-2023 年 10 月 22 日 **2023 年第 42 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 496 个，其中高危漏洞 192 个、中危漏洞 271 个、低危漏洞 33 个。漏洞平均分值为 6.17。本周收录的漏洞中，涉及 0day 漏洞 437 个（占 88%），其中互联网上出现“Cisco IOS XE Software web UI 权限提升漏洞、Netis N3Mv2 缓冲区溢出漏洞”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 11677 个，与上周（19726 个）环比减少 41%。

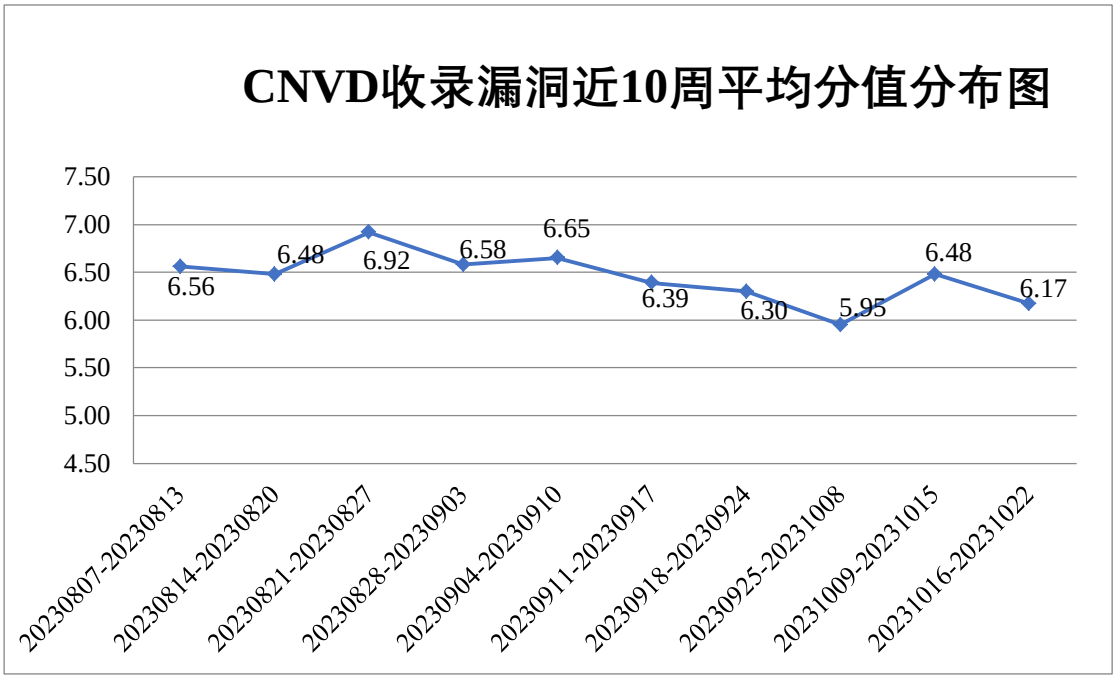

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 32 起，向基础电

信企业通报漏洞事件 11 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 1152 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 156 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 68 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、重庆中联信息产业有限责任公司、重庆国翰能源发展有限公司、中银金融科技有限公司、中天城投集团物业管理有限公司、中汽数据有限公司、中国邮政速递物流股份有限公司、中版文化传播有限公司、智业软件股份有限公司、智业互联（厦门）健康科技有限公司、智互联（深圳）科技有限公司、郑州市金水区恒友摄影软件经营部、郑州力通水务有限公司、浙江宇视科技有限公司、漳州市芗城帝兴软件开发有限公司、云内控科技有限公司、云南云才人力资源咨询有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、盈富量化信息技术有限公司、兄弟（中国）商业有限公司、西安众邦网络科技有限公司、武汉微问网络科技有限公司、武汉天地伟业科技有限公司、武汉今客软件有限公司、武汉富思特创新信息技术有限公司、无锡一族科技有限公司、网件（北京）网络技术有限公司、万兴科技集团股份有限公司、万商云集（成都）科技股份有限公司、外语教学与研究出版社有限责任公司、同望科技股份有限公司、同程网络科技股份有限公司、天闻数媒科技（北京）有限公司、天地伟业技术有限公司、天宝莅德电子科技（上海）有限公司北京分公司、太原易思软件技术有限公司、苏州巨细信息科技有限公司、四川迅睿云软件开发有限公司、深圳银澎云计算有限公司、深圳市知学云科技有限公司、深圳市通恒伟创科技有限公司、深圳市思迅软件股份有限公司、深圳市敏捷智盛网络有限公司、深圳市美科星通信技术有限公司、深圳市科荣软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市国信合成科技有限公司、深圳市道尔智控科技股份有限公司、深圳市安盟信息科技有限公司、深圳华视美达信息技术有限公司、深信服科技股份有限公司、申瓯通信设备有限公司、上海装盟信息科技有限公司、上海万欣计算机信息科技有限公司、上海树维信息科技有限公司、上海穆云智能科技有限公司、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、上海伯俊软件科技有限公司、上海爱数信息技术股份有限公司、陕西小伙伴网络科技有限公司、山东五征集团有限公司、山东潍大软件有限公司、山东山大电力技术股份有限公司、厦门四信通信科技有限公司、厦门科拓通讯技术股份有限公司、润申信息科技（上海）有限公司、瑞纳智能设备股份有限公司、锐珂（上海）医疗器材有限公司、青岛聚城网络科技有限公司、普联技术有限公司、鹏为软件股份有限公司、诺盾科技有限公司、南宁迈世信息技术有限公司、南京涌亿思信息技术有限公司、迈普通信技术股份有限公司、临沂科锐电子有限公司、理光（中国）投资有限公司、乐山易通天下网络科技有限公司、廊坊市极致网络科技有限公司、蓝网科技股份有限公司、江苏绿港现代

农业发展股份有限公司、江苏冠宇科技集团有限公司、济南沐阳信息技术有限公司、吉翁电子（深圳）有限公司、淮南市银泰软件科技有限公司、湖北点点点科技有限公司、洪湖尔创网联信息技术有限公司、河南中翎工程建设有限公司、和宇健康科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州先锋电子技术股份有限公司、杭州叁体网络科技有限公司、杭州海康威视数字技术股份有限公司、海南道仁网络科技有限公司、海口快推科技有限公司、国交信息股份有限公司、贵州永恒光科技有限公司、广州讯尔软件科技有限公司、广州图创计算机软件开发有限公司、广州速盈信息科技有限公司、广州思迈特软件有限公司、广州市天翎网络科技有限公司、广州市欢雀科技有限公司、广州科税信息科技有限公司、广州华的网络科技有限公司、广州恒企教育科技有限公司、广州鼎甲计算机科技有限公司、广西青椰网络科技有限公司、广联达科技股份有限公司、广东飞企互联科技股份有限公司、福建银达汇智信息科技股份有限公司、东莞市智跃软件科技有限公司、鼎捷软件股份有限公司、大连金马衡器有限公司、大连富豪科技有限公司、大华（集团）有限公司、达索析统（上海）信息技术有限公司、传化上合（青岛）国际经贸有限公司、成都虚谷伟业科技有限公司、成都天问互联科技有限公司、成都任我行软件股份有限公司、彩讯科技股份有限公司、采采网络技术有限公司、北京中盈安信技术服务股份有限公司、北京中科聚网信息技术有限公司、北京致远互联软件股份有限公司、北京正影网络科技有限公司、北京泽元迅长软件有限公司、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、北京象新力科技有限公司、北京通达信科科技有限公司、北京硕人时代科技股份有限公司、北京启明星辰信息安全技术有限公司、北京派网软件有限公司、北京迷彩虎科技有限公司、北京猎鹰安全科技有限公司、北京久其软件股份有限公司、北京京东叁佰陆拾度电子商务有限公司、北京金盘鹏图软件技术有限公司、北京金和网络股份有限公司、北京飞书科技有限公司、北京创新乐知网络技术有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、北京安信立融科技股份有限公司、奥丁创新科技（吉林）有限公司、安徽旭帆信息科技有限公司和 Sapido Technology Inc。

本周，CNVD 发布了《Oracle 发布 2023 年 10 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9386

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、天津市国瑞数码安全系统股份有限公司、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。亚信科技（成都）有限公司、奇安星城网络安全运营服务（长沙）有限公司、杭州美创科技有限公司、联想集团、

快页信息技术有限公司、安徽锋刃信息科技有限公司、河南东方云盾信息技术有限公司、内蒙古洞明科技有限公司、湖南泛联新安信息科技有限公司、工业和信息化部电子第五研究所-数据治理服务中心、北京君云天下科技有限公司、星云博创科技有限公司、合肥梆梆信息科技有限公司、赛尔网络有限公司、杭州默安科技有限公司、江苏天竞云合数据技术有限公司、杭州飞致云信息科技有限公司、河南悦海数安科技有限公司、北京网御星云信息技术有限公司、北京中关村实验室、江西和尔惠信息技术有限公司、江苏晟晖信息科技有限公司、杭州海康威视数字技术股份有限公司、超聚变数字技术有限公司、中国工商银行、成都安美勤信息技术股份有限公司、北京微步在线科技有限公司、北京天防安全科技有限公司、中孚安全技术有限公司、北京华顺信安信息技术有限公司、浙江东安检测技术有限公司、南方电网数字电网集团信息通信科技有限公司、汇安云（山东）信息科技有限公司、北京时代新威信息技术有限公司、中国电信股份有限公司上海研究院、上海直画科技有限公司、博智安全科技股份有限公司、浙江中控技术股份有限公司、国网信息通信产业集团有限公司、成都天天网安信息安全技术有限公司、上海亿保健康科技集团有限公司、河南灵创电子科技有限公司、山东新潮信息技术有限公司、北京远禾科技有限公司、成都卓越华安信息技术服务有限公司、广州安亿信软件科技有限公司、苏州棱镜七彩信息科技有限公司及其他个人白帽子向 CNVD 提交了 11677 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 8638 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）	5037	5037
斗象科技（漏洞盒子）	2863	2863
北京天融信网络安全技术有限公司	799	42
天津市国瑞数码安全系统股份有限公司	786	0
新华三技术有限公司	535	0
上海交大	467	467
安天科技集团股份有限公司	301	1
北京神州绿盟科技有限公司	291	291
深信服科技股份有限	275	0

公司		
三六零数字安全科技集团有限公司	271	271
阿里云计算有限公司	107	8
北京启明星辰信息安全技术有限公司	82	0
杭州安恒信息技术股份有限公司	49	2
北京知道创宇信息技术有限公司	45	0
中电科网络安全科技股份有限公司	36	36
南京联成科技发展股份有限公司	19	19
杭州迪普科技股份有限公司	14	0
贵州泰若数字科技有限公司	9	9
京东科技信息技术有限公司	5	5
北京长亭科技有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	1	1
亚信科技（成都）有限公司	452	452
奇安星城网络安全运营服务（长沙）有限公司	182	182
杭州美创科技有限公司	133	133
联想集团	79	79
快页信息技术有限公司	55	55

安徽锋刃信息科技有限公司	35	35
河南东方云盾信息技术有限公司	21	21
内蒙古洞明科技有限公司	12	12
湖南泛联新安信息科技有限公司	11	11
工业和信息化部电子第五研究所-数据治理服务中心	9	9
北京君云天下科技有限公司	7	7
星云博创科技有限公司	6	6
合肥梆梆信息科技有限公司	6	6
赛尔网络有限公司	5	5
杭州默安科技有限公司	5	5
江苏天竞云合数据技术有限公司	5	5
杭州飞致云信息科技有限公司	4	4
河南悦海数安科技有限公司	4	4
北京网御星云信息技术有限公司	4	4
北京中关村实验室	3	3
江西和尔惠信息技术有限公司	3	3
江苏晟晖信息科技有限公司	2	2
杭州海康威视数字技术股份有限公司	2	2

超聚变数字技术有限公司	2	2
中国工商银行	2	2
成都安美勤信息技术股份有限公司	2	2
北京微步在线科技有限公司	2	2
北京天防安全科技有限公司	2	2
中孚安全技术有限公司	2	2
北京华顺信安信息技术有限公司	1	1
浙江东安检测技术有限公司	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
汇安云（山东）信息科技有限公司	1	1
北京时代新威信息技术有限公司	1	1
中国电信股份有限公司上海研究院	1	1
上海直画科技有限公司	1	1
博智安全科技股份有限公司	1	1
浙江中控技术股份有限公司	1	1
国网信息通信产业集团有限公司	1	1
成都天天网安信息安全技术有限公司	1	1
上海亿保健康科技集	1	1

团有限公司		
河南灵创电子科技有限公司	1	1
山东新潮信息技术有限公司	1	1
北京远禾科技有限公司	1	1
成都卓越华安信息技术服务有限公司	1	1
广州安亿信软件科技有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
CNCERT 广西分中心	5	5
CNCERT 河北分中心	5	5
个人	1537	1537
报送总计	14617	11677

本周漏洞按类型和厂商统计

本周，CNVD 收录了 496 个漏洞。WEB 应用 250 个，应用程序 118 个，网络设备（交换机、路由器等网络端设备）100 个，安全产品 12 个，操作系统 7 个，智能设备（物联网终端设备）7 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
WEB 应用	250
应用程序	118
网络设备（交换机、路由器等网络端设备）	100
安全产品	12
操作系统	7
智能设备（物联网终端设备）	7
数据库	2

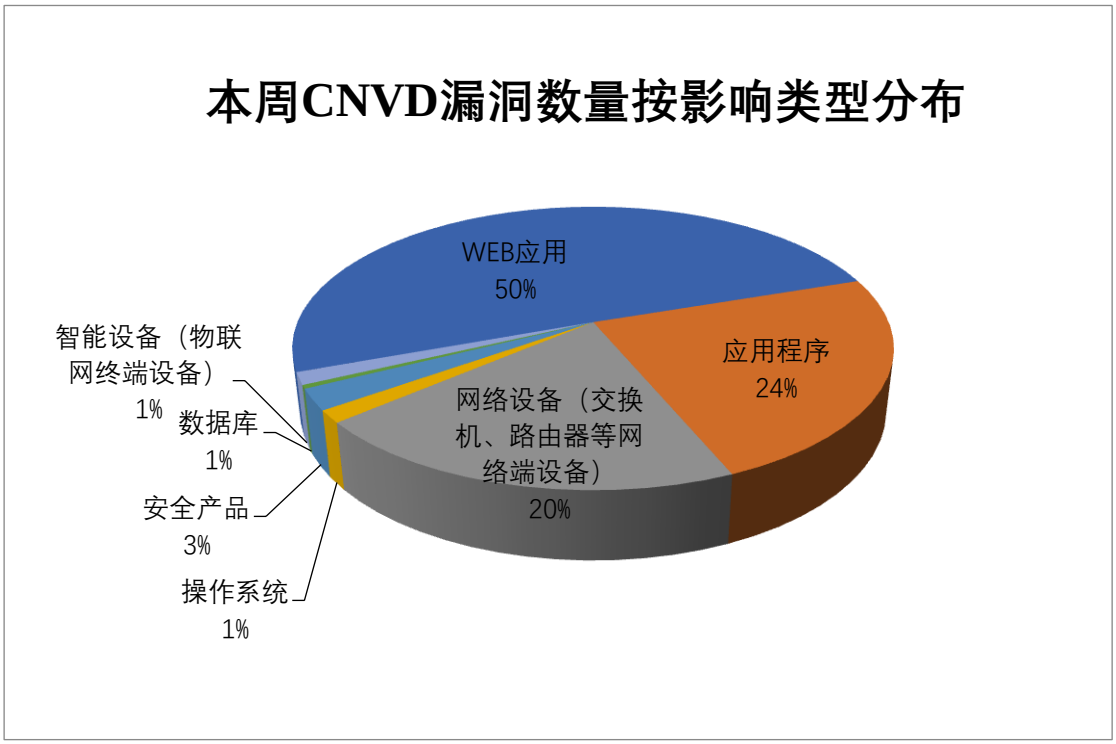

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、北京百卓网络技术有限公司、WordPress 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	18	3%
2	北京百卓网络技术有限公司	15	3%
3	WordPress	14	3%
4	DELL	12	2%
5	Adobe	11	2%
6	安徽青柿信息科技有限公司	9	2%
7	Microsoft	8	2%
8	IBM	8	2%
9	新华三技术有限公司	8	2%
10	其他	393	79%

本周行业漏洞收录情况

本周，CNVD 收录了 62 个电信行业漏洞，56 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Huawei HarmonyOS 和 EMUI 类型混肴漏洞、Rockwell Automation FactoryTalk Linx 输入验证错误漏洞”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/

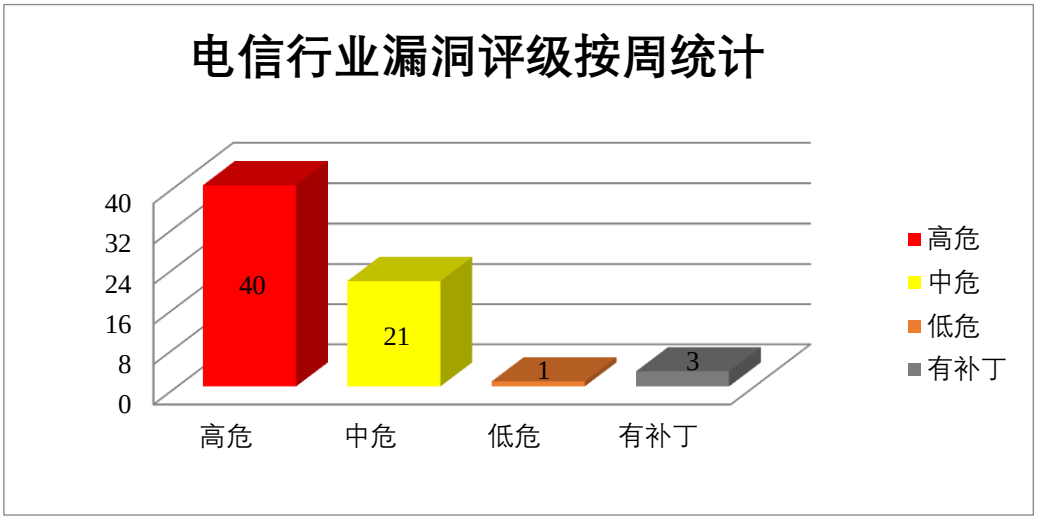

图 3 电信行业漏洞统计

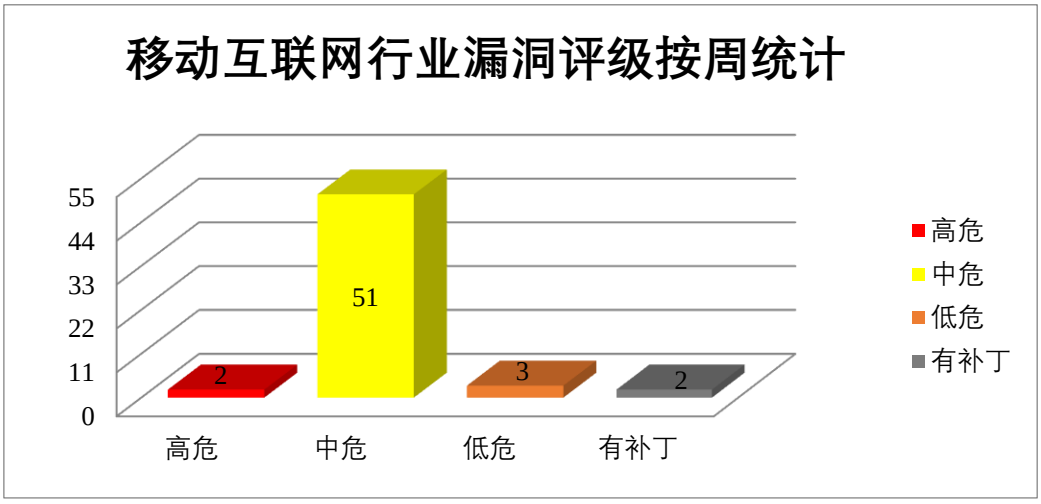

图 4 移动互联网行业漏洞统计

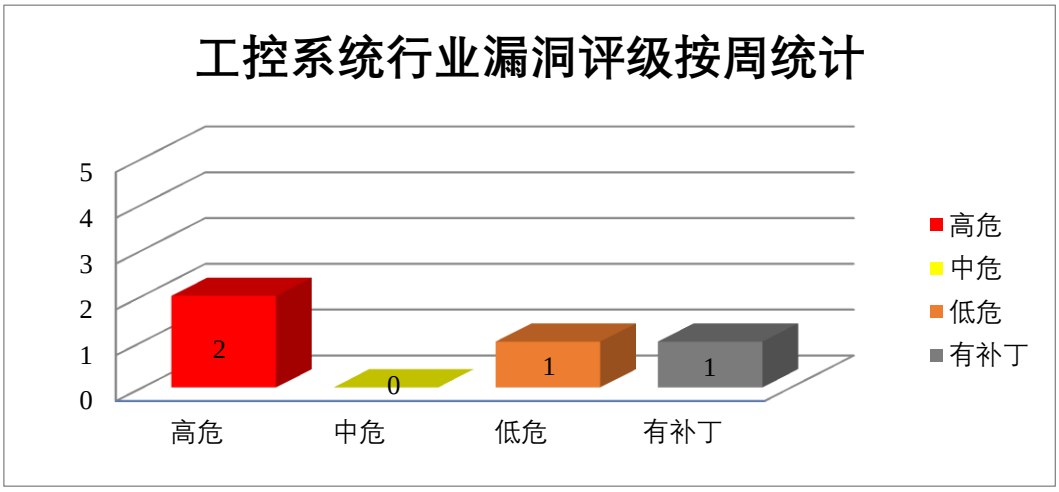

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Edge 是美国微软（Microsoft）公司的一款 Windows 10 之后版本系统附带的 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上获取更高的权限。

CNVD 收录的相关漏洞包括：Microsoft Edge 权限提升漏洞（CNVD-2023-76758、CNVD-2023-76759、CNVD-2023-76760、CNVD-2023-76761、CNVD-2023-76762、CNVD-2023-76763、CNVD-2023-76764、CNVD-2023-76765）。其中，除“Microsoft Edge 权限提升漏洞（CNVD-2023-76762、CNVD-2023-76763）”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-2023-76758
https://www.cnvd.org.cn/flaw/show/CNVD-2023-76759
https://www.cnvd.org.cn/flaw/show/CNVD-2023-76760
https://www.cnvd.org.cn/flaw/show/CNVD-2023-76761
https://www.cnvd.org.cn/flaw/show/CNVD-2023-76762
https://www.cnvd.org.cn/flaw/show/CNVD-2023-76763
https://www.cnvd.org.cn/flaw/show/CNVD-2023-76764
https://www.cnvd.org.cn/flaw/show/CNVD-2023-76765

2、IBM 产品安全漏洞

IBM Aspera 是美国国际商业机器（IBM）公司的一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。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特制的 XML 输入获取敏感的凭据信息，导致缓冲区溢出并在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Aspera Cargo and IBM Aspera Connect 信息泄露漏洞、IBM Aspera Faspex 信息泄露漏洞（CNVD-2023-76768、CNVD-2023-76766、CNVD-2023-76773）、IBM Aspera Faspex 安全绕过漏洞、IBM Aspera Cargo and IBM Aspera Connect 代码执行漏洞（CNVD-2023-76772、CNVD-2023-76771）、IBM Aspera Connect and IBM Aspera Cargo 缓冲区溢出漏洞。其中，“IBM Aspera Cargo and IBM Aspera Connect 代码执行漏洞（CNVD-2023-76772、CNVD-2023-76771）、IBM Aspera Connect and IBM Aspera Cargo 缓冲区溢出漏洞”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-2023-76769

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76768

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76767

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76766

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76773

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76772

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76771

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76770

3、Adobe 产品安全漏洞

Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。Adobe Bridge 是一款功能强大的创意资源管理器，可让用户快速轻松地预览、组织、编辑和发布多个创意资源，编辑元数据，为素材资源添加关键字、标签和评分。Adobe Bridge 使用集合组织资产，并使用强大的过滤器和高级元数据搜索功能查找资产。Adobe Illustrator 是一套基于向量的图像制作软件。Adobe After Effects 是一套视觉效果和动态图形制作软件，该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。Adobe InDesign 是一套排版编辑应用程序。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 ASLR 等缓解措施，导致敏感内存泄露，导致缓冲区溢出或堆溢出，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 Photoshop 缓冲区溢出漏洞（CNVD-2023-76927）、Adobe Bridge 越界读取漏洞（CNVD-2023-76928）、Adobe Illustrator 缓冲区溢出漏洞（CNVD-2023-76932、CNVD-2023-76930、CNVD-2023-76935、CNVD-2023-76933）、Adobe After Effects 越界读取漏洞（CNVD-2023-76938）、Adobe InDesign 缓冲区溢出漏洞（CNVD-2023-76940）。其中，除“Adobe Bridge 越界读取漏洞（CNVD-2023-76928）”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-2023-76927

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76928

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76932

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76930

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76935

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76933

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76938

https://www.cnvd.org.cn/flaw/show/CNVD-2023-76940

4、DELL 产品安全漏洞

Dell SmartFabric Storage Software 是美国戴尔（Dell）公司的一个独立的存储软件解决方案。Dell Wyse Management Suite 是一套用于管理和优化 Wyse 端点的、可扩展的解决方案。该产品包括 Wyse 端点集中管理、资产追踪和自动设备发现等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取写入日志文件的敏感信息，导致未经授权的数据访问，在系统上执行任意命令等。

CNVD 收录的相关漏洞包括：Dell SmartFabric storage software 命令注入漏洞、Dell SmartFabric Storage Software 输入验证错误漏洞、Dell SmartFabric Storage Software 权限提升漏洞、Dell SmartFabric Storage Software 路径遍历漏洞、Dell SmartFabric Storage Software 访问控制错误漏洞、Dell SmartFabric Storage Software 操作系统命令注入漏洞（CNVD-2023-77958、CNVD-2023-78231）、Dell Wyse Management Suite 信息泄露漏洞。其中，“Dell SmartFabric storage software 命令注入漏洞、Dell SmartFabric Storage Software 权限提升漏洞、Dell SmartFabric Storage Software 操作系统命令注入漏洞”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-2023-77953
https://www.cnvd.org.cn/flaw/show/CNVD-2023-77954
https://www.cnvd.org.cn/flaw/show/CNVD-2023-77955
https://www.cnvd.org.cn/flaw/show/CNVD-2023-77956
https://www.cnvd.org.cn/flaw/show/CNVD-2023-77957
https://www.cnvd.org.cn/flaw/show/CNVD-2023-77958
https://www.cnvd.org.cn/flaw/show/CNVD-2023-78231
https://www.cnvd.org.cn/flaw/show/CNVD-2023-78233

5、D-Link DIR-806 命令执行漏洞

D-Link DIR-806 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-806 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-2023-78314

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-2023-76758	Microsoft Edge 权限提升漏洞（CNVD-2023-76758）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36562

CNVD-2023-76759	Microsoft Edge 权限提升漏洞（CNVD-2023-76759）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36735
CNVD-2023-76772	IBM Aspera Cargo and IBM Aspera Connect 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://www.ibm.com/support/pages/node/6966588
CNVD-2023-76771	IBM Aspera Cargo and IBM Aspera Connect 代码执行漏洞（CNVD-2023-76771）	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/6966588
CNVD-2023-76930	Adobe Illustrator 缓冲区溢出漏洞（CNVD-2023-76930）	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-2023-76935	Adobe Illustrator 缓冲区溢出漏洞（CNVD-2023-76935）	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-2023-77953	Dell SmartFabric storage software 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.dell.com/support/kbdoc/en-us/000201667/dsa-2022-156-dell-emc-smartfabric-storage-software-security-update-for-multiple-component-vulnerabilities
CNVD-2023-78236	TOTOLINK X5000R 和 A7000R UploadCustomModule 函数堆栈溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/
CNVD-2023-78238	TOTOLINK X5000R 和 A7000R setLanguageCfg 函数堆栈溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/
CNVD-2023-78312	Rockwell Automation FactoryTalk Linx 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1141040

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上获取更高的权限。此外，IBM、Adobe、Dell 等多款产品被披露存在多个漏洞，攻击者可利用漏洞读取写入日志文件的敏感信息，使用特制的 XML 输入获取敏感的凭据信息，导致缓冲区溢出或堆溢出，在当前用户的上下文中执行任意代码等。另外，D-Link DIR-806 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、Netis N3Mv2 缓冲区溢出漏洞

验证描述

Netis N3Mv2 是一款路由器设备。

Netis N3Mv2 存在缓冲区溢出漏洞，攻击者可利用该漏洞通过在 hostName 参数中发送特制请求，导致拒绝服务。

验证信息

POC 链接：https://github.com/adhikara13/CVE/blob/main/netis_N3/buffer%20overflow%20in%20hostname%20parameter%20leads%20to%20DOS.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-78310

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. 开源 CasaOS 云软件中发现安全漏洞

攻击者可以成功利用开源 CasaOS 个人云软件中发现的两个安全漏洞来实现任意代码执行并接管易受攻击的系统。

参考链接：https://thehackernews.com/2023/10/critical-vulnerabilities-uncovered-in.html

2. WIKI 系统 Confluence 存在安全漏洞

近日，CISA、FBI 和 MS-ISAC 提醒网络管理员为其 Atlassian Confluence 服务器更新安全补丁，以防止网络攻击者中主动利用漏洞 CVE-2023-22515。

参考链接：https://www.freebuf.com/news/381032.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