国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 11 月 14 日-2022 年 11 月 20 日 **2022 年第 46 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 622 个，其中高危漏洞 228 个、中危漏洞 323 个、低危漏洞 71 个。漏洞平均分值为 6.10。本周收录的漏洞中，涉及 0day 漏洞 411 个（占 66%），其中互联网上出现“Tenda AX 180 堆栈溢出漏洞、Delight Nashorn Sandbox 拒绝服务漏洞”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 17037 个，与上周（18262 个）环比减少 7%。

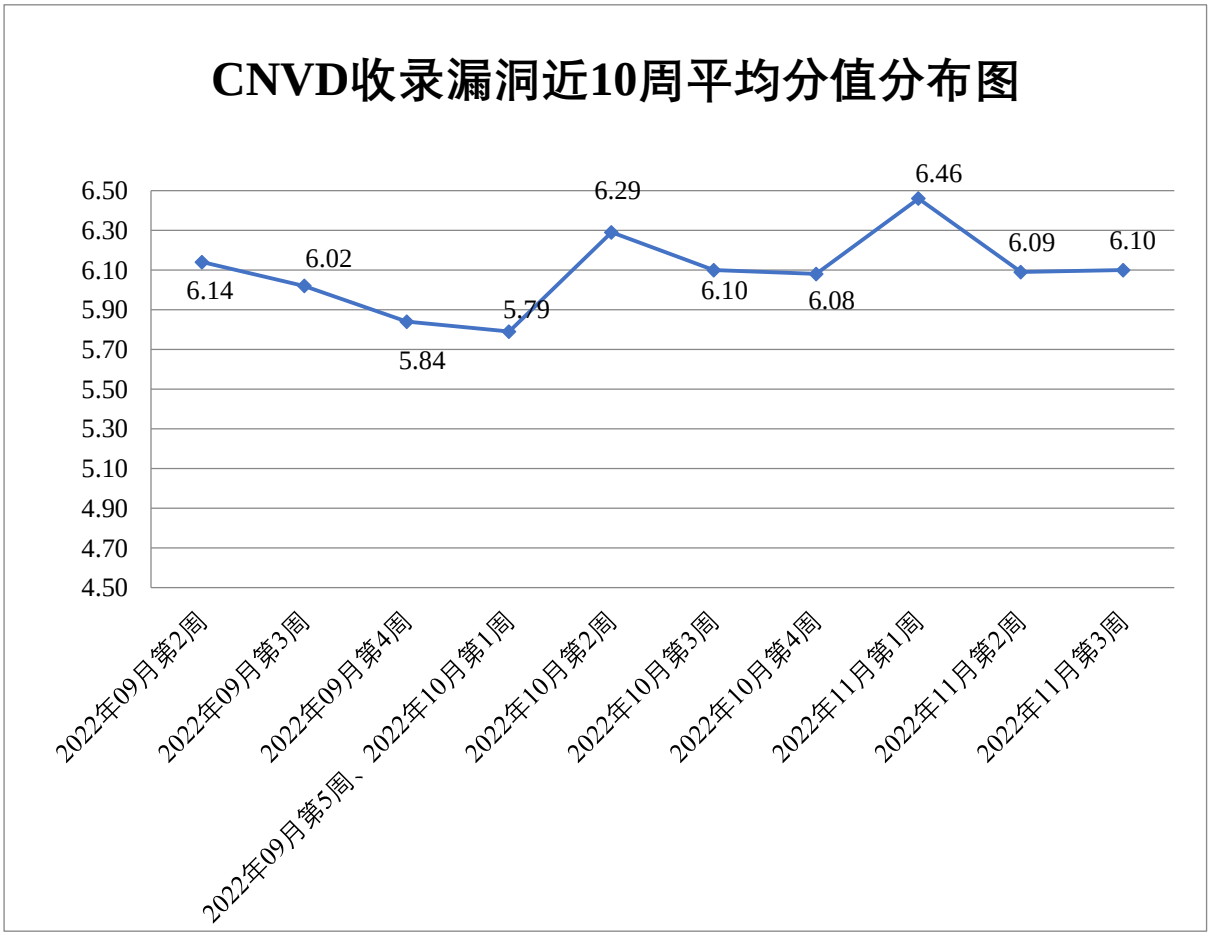

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 43 起，向基础电信企业通报漏洞事件 27 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 1014 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 207 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 144 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、重庆梅安森科技股份有限公司、中健康（北京）高血压医疗科技有限公司、智互联（深圳）科技有限公司、正泰集团股份有限公司、浙江零跑科技股份有限公司、浙江禾成云计算有限公司、浙江大华技术股份有限公司、长沙市同迅计算机科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、赢火虫软件科技（上海）有限公司、熊猫智慧水务有限公司、新疆云景网络科技有限公司、小明太极（湖北）国漫文化有限公司、夏普商贸（中国）有限公司、武汉中地数码科技有限公司、武汉小药药医药科技有限公司、武汉秒开网络科技有限公司、同方健康科技（北京）股份有限公司、天地伟业技术有限公司、泰安云豹网络科技有限公司、台达集团、苏州遇见信息科技有限公司、苏州天一信德环保科技有限公司、苏州瑞立思科技有限公司、苏州科达科技股份有限公司、苏州汇川技术有限公司、搜狗公司、四川迅游网络科技股份有限公司、四川天邑康和通信股份有限公司、沈阳卡得智能科技有限公司、深圳坐标软件集团有限公司、深圳希施玛数据科技有限公司、深圳维盟科技股份有限公司、深圳市讯视安科技有限公司、深圳市信锐网科技术有限公司、深圳市西迪特科技有限公司、深圳市思迅软件股份有限公司、深圳市科漫达智能管理科技有限公司、深圳市吉祥腾达科技有限公司、深圳市宏电技术股份有限公司、深圳市鼎游信息技术有限公司、深圳市博思协创网络科技有限公司、深圳科士达科技股份有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海展盟网络科技有限公司、上海银宇信息技术有限公司、上海携程商务有限公司、上海仙蒂网络科技有限公司、上海威派格智慧水务股份有限公司、上海淞泓智能汽车科技有限公司、上海盛代信息科技有限公司、上海锐昉科技有限公司、上海锐道信息技术有限公司、上海凌灼信息科技有限公司、上海居亦科技发展有限公司、上海华测导航技术股份有限公司、上海汉得信息技术股份有限公司、上海泛微网络科技股份有限公司、上海步科自动化股份有限公司、上海博达数据通信有限公司、熵基科技股份有限公司、山西万鸿科技有限公司、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、山东天虹同济

信息技术有限公司、山东欧倍尔软件科技有限责任公司、山东金钟科技集团股份有限公司、山东环球软件股份有限公司、山东博硕自动化技术有限公司、厦门四信通信科技有限公司、厦门四联信息技术有限公司、厦门零一世界科技有限公司、全城淘信息技术服务有限公司、清枫（北京）科技有限公司、七友科技股份有限公司、普联技术有限公司、尼康映像仪器销售（中国）有限公司、南宁迈世信息技术有限公司、南宁火蝶科技有限公司、南京涌亿思信息技术有限公司、南京帆软软件有限公司、南京偲言睿网络科技有限公司、梦想 CMS、美图公司、美国菲力尔公司、迈普通信技术股份有限公司、朗坤智慧科技股份有限公司、狂雨小说 cms、江西兴泰科技股份有限公司、江西铭软科技有限公司、江苏省广电有线信息网络股份有限公司、江苏灵匠信息科技有限公司、佳能（中国）有限公司、济南中维世纪科技有限公司、济南便装网网络科技有限公司、吉翁电子（深圳）有限公司、霍州煤电集团鑫钜煤机装备制造有限责任公司、惠普贸易（上海）有限公司、华夏 ERP、湖南壹拾捌号网络技术有限公司、湖南强智科技发展有限公司、湖南康通电子股份有限公司、湖南建研信息技术股份有限公司、湖南翱云网络科技有限公司、湖北楚天智能交通股份有限公司、河南省南阳市人民政府办公室、河南斧牛网络科技有限公司、杭州易紧通电子商务有限公司、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、杭州三汇数字信息技术有限公司、杭州迦智科技有限公司、杭州吉拉科技有限公司、杭州海康威视数字技术股份有限公司、杭州冠航科技有限公司、杭州迪普科技股份有限公司、广州网易计算机系统有限公司、广州宁静海信息科技有限公司、广州好象科技有限公司、广州点步信息科技有限公司、广州安网通信技术有限公司、广联达科技股份有限公司、福州联迅信息科技有限公司、烽火通信科技股份有限公司、飞天站群系统、东华软件股份公司、得力集团有限公司、大连华天软件有限公司、创维集团有限公司、成都索贝数码科技股份有限公司、成都傲梅科技有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京五一搜搜软件科技有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京世纪超星信息技术发展有限责任公司、北京七心云科技有限公司、北京派网软件有限公司、北京联达动力信息科技股份有限公司、北京九思协同软件有限公司、北京京东叁佰陆拾度电子商务有限公司、北京环球医康咨询服务有限公司、北京国炬信息技术有限公司 、北京弹幕网络科技有限公司、北京超图软件股份有限公司、北京必胜课教育科技有限公司、北京百卓网络技术有限公司、安徽阳光心健科技发展有限公司、安徽皖通邮电股份有限公司、阿里巴巴集团安全应急响应中心、zzzcms、seacms、phpMyAdmin、NETGEAR、Flir Systems Inc、ClassCMS 和 BEESCMS。

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、北京神州

绿盟科技有限公司、安天科技集团股份有限公司、新华三技术有限公司、南京众智维信息科技有限公司等单位报送公开收集的漏洞数量较多。北京升鑫网络科技有限公司、北京山石网科信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、博智安全科技股份有限公司、杭州默安科技有限公司、快页信息技术有限公司、河南东方云盾信息技术有限公司、杭州迪普科技股份有限公司、浙江木链物联网科技有限公司、苏州棱镜七彩信息科技有限公司、河南信安世纪科技有限公司、山东新潮信息技术有限公司、山石网科通信技术股份有限公司、山东云天安全技术有限公司、河南灵创电子科技有限公司、北京水木羽林科技有限公司、北京微步在线科技有限公司、安徽锋刃信息科技有限公司、北京华顺信安信息技术有限公司、贵州多彩网安科技有限公司、江苏保旺达软件技术有限公司、浙江大华技术股份有限公司、奇安星城网络安全运营服务（长沙）有限公司、星云博创科技有限公司、重庆都会信息科技有限公司、内蒙古信元网络安全技术股份有限公司、安徽长泰科技有限公司、蚂蚁金服、上海天存信息技术有限公司、杭州美创科技有限公司、上海电器科学研究所（集团）有限公司、广州安亿信软件科技有限公司、江苏网擎信息技术有限公司、银华基金管理股份有限公司、中国电信股份有限公司网络安全产品运营中心、贵州电网有限责任公司信息中心、北京君云天下科技有限公司、重庆易阅科技有限公司、北京华云安信息技术有限公司、有度网络安全技术有限公司、国网湖北省电力有限公司恩施供电公司、广东唯顶信息科技股份有限公司、上海迅御安全科技有限公司、西安敏恒信息技术有限公司、河南迪富信息股份有限公司、华泰保险集团股份有限公司、陕西青山四纪信息技术有限公司、上海纽盾科技股份有限公司、北京安帝科技有限公司、苏州众里数码科技有限公司及其他个人白帽子向 CNVD 提交了 17037 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）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 13610 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）	9733	9733
奇安信网神（补天平台）	2556	2556
上海交大	1027	1027
北京启明星辰信息安全技术有限公司	630	2
北京神州绿盟科技有限公司	506	220
三六零数字安全科技集团有限公司	294	294

安天科技集团股份有限公司	270	0
新华三技术有限公司	259	0
南京众智维信息科技有限公司	221	221
深信服科技股份有限公司	213	1
西安四叶草信息技术有限公司	183	183
北京数字观星科技有限公司	171	0
杭州安恒信息技术股份有限公司	158	119
北京天融信网络安全技术有限公司	106	4
恒安嘉新（北京）科技股份公司	103	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	31	4
中国电信集团系统集成有限责任公司	29	2
京东科技信息技术有限公司	19	6
卫士通信息产业股份有限公司	17	17
内蒙古云科数据服务股份有限公司	13	13
远江盛邦（北京）网络安全科技股份有限公司	1	1
北京升鑫网络科技有限公司	480	480
北京山石网科信息技	205	205

术有限公司		
北京云科安信科技有限公司（Seraph 安全实验室）	183	183
博智安全科技股份有限公司	51	51
杭州默安科技有限公司	37	37
快页信息技术有限公司	31	31
河南东方云盾信息技术有限公司	20	20
杭州迪普科技股份有限公司	19	5
浙江木链物联网科技有限公司	18	18
苏州棱镜七彩信息科技有限公司	11	11
河南信安世纪科技有限公司	11	11
山东新潮信息技术有限公司	10	10
山石网科通信技术股份有限公司	10	10
山东云天安全技术有限公司	9	9
河南灵创电子科技有限公司	9	9
北京水木羽林科技有限公司	9	9
北京微步在线科技有限公司	8	8
安徽锋刃信息科技有限公司	8	8
北京华顺信安信息技	7	7

术有限公司		
贵州多彩网安科技有限公司	7	7
江苏保旺达软件技术有限公司	7	7
浙江大华技术股份有限公司	5	5
奇安星城网络安全运营服务（长沙）有限公司	5	5
星云博创科技有限公司	5	5
重庆都会信息科技有限公司	4	4
内蒙古信元网络安全技术股份有限公司	4	4
安徽长泰科技有限公司	4	4
蚂蚁金服	3	3
上海天存信息技术有限公司	3	3
杭州美创科技有限公司	2	2
上海电器科学研究所（集团）有限公司	2	2
广州安亿信软件科技有限公司	2	2
江苏网擎信息技术有限公司	2	2
银华基金管理股份有限公司	2	2
中国电信股份有限公司网络安全产品运营中心	1	1
贵州电网有限责任公	1	1

司信息中心		
北京君云天下科技有限公司	1	1
重庆易阅科技有限公司	1	1
北京华云安信息技术有限公司	1	1
有度网络安全技术有限公司	1	1
国网湖北省电力有限公司恩施供电公司	1	1
广东唯顶信息科技股份有限公司	1	1
上海迅御安全科技有限公司	1	1
西安敏恒信息技术有限公司	1	1
河南迪富信息股份有限公司	1	1
华泰保险集团股份有限公司	1	1
陕西青山四纪信息技术有限公司	1	1
上海纽盾科技股份有限公司	1	1
北京安帝科技有限公司	1	1
苏州众里数码科技有限公司	1	1
CNCERT 湖南分中心	8	8
CNCERT 福建分中心	4	4
CNCERT 宁夏分中心	2	2
个人	1425	1425
报送总计	19247	17037

本周漏洞按类型和厂商统计

本周，CNVD 收录了 622 个漏洞。WEB 应用 237 个，应用程序 223 个，网络设备（交换机、路由器等网络端设备）110 个，智能设备（物联网终端设备）27 个，操作系统 14 个，安全产品 8 个，数据库 3 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	237
应用程序	223
网络设备（交换机、路由器等网络端设备）	110
智能设备（物联网终端设备）	27
操作系统	14
安全产品	8
数据库	3

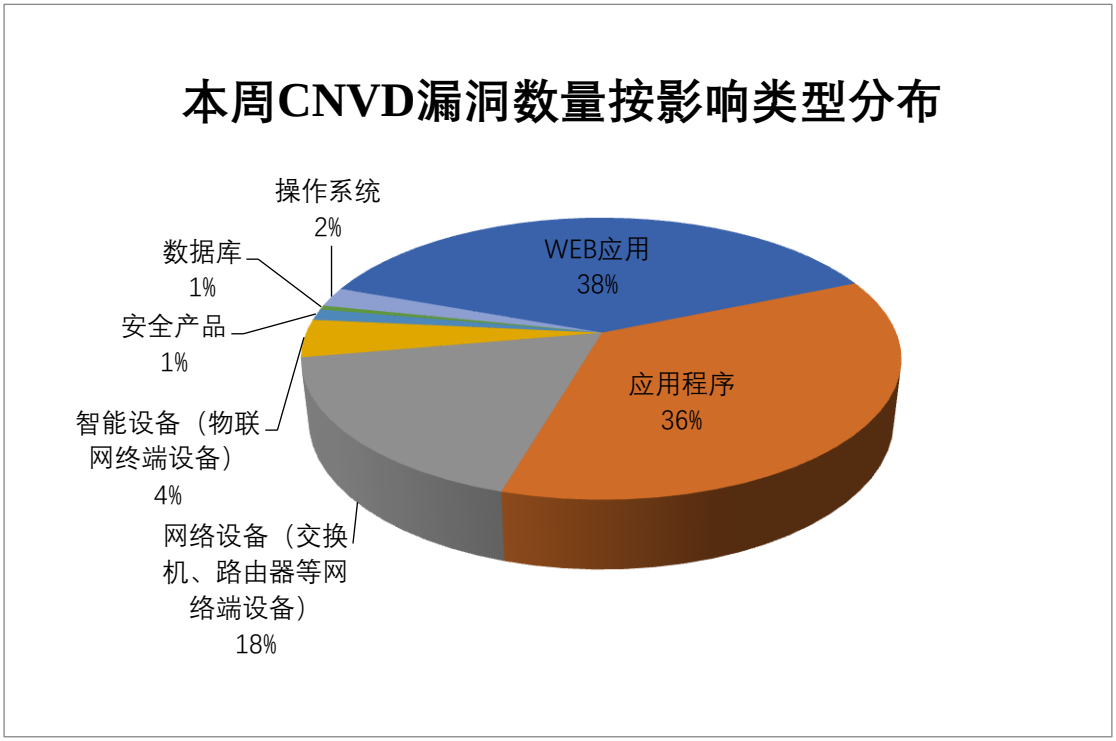

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tenda、IBM、Cesanta 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	Tenda	40	8%
2	IBM	19	3%

3	Cesanta	15	2%
4	F5	14	2%
5	北京百卓网络技术有限公司	12	2%
6	Google	12	2%
7	Microsoft	11	2%
8	Adobe	10	1%
9	TOTOLINK	9	1%
10	其他	480	77%

本周行业漏洞收录情况

本周，CNVD 收录了 75 个电信行业漏洞，32 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，“Tenda AC1206 缓冲区溢出漏洞 、Google Android 缺少授权漏洞（CNVD-2022-78153）、Mitsubishi Electric MELSEC-Q Series 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/

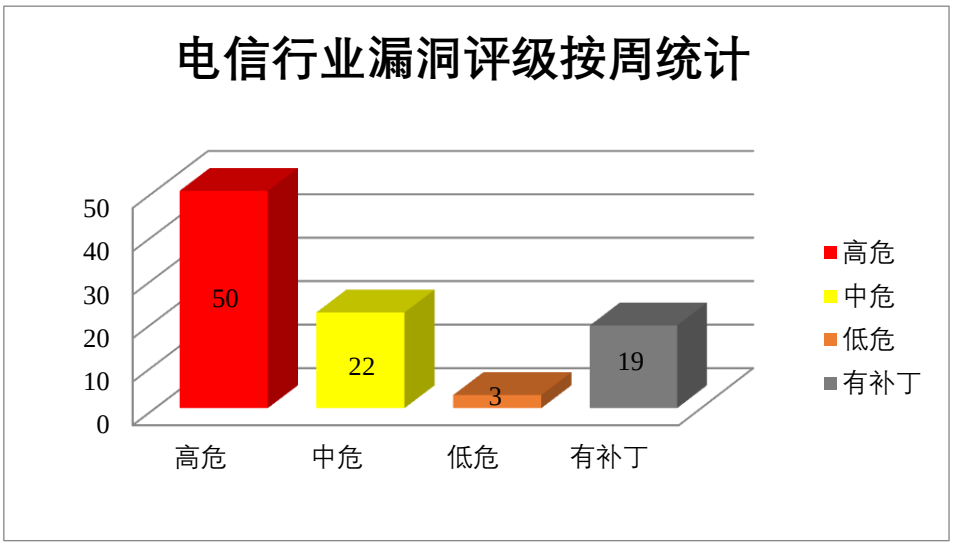

图 3 电信行业漏洞统计

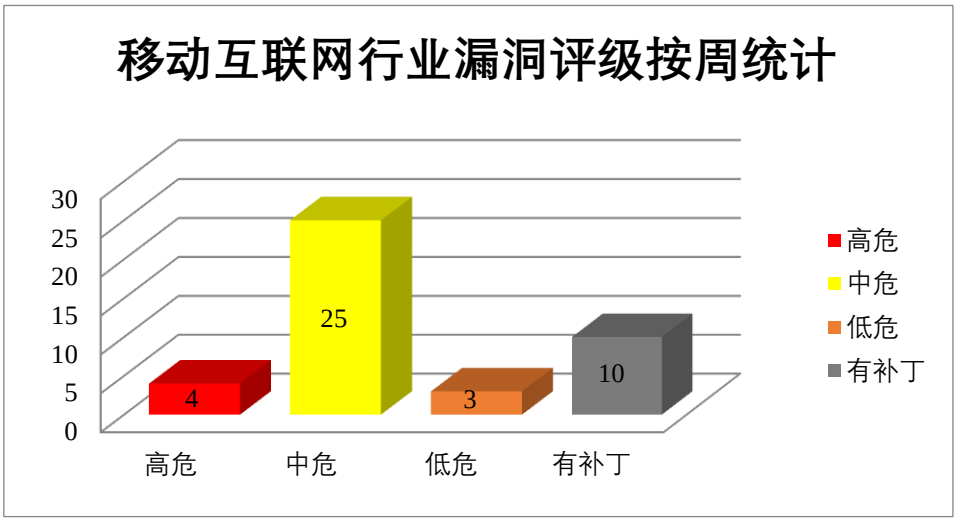

图 4 移动互联网行业漏洞统计

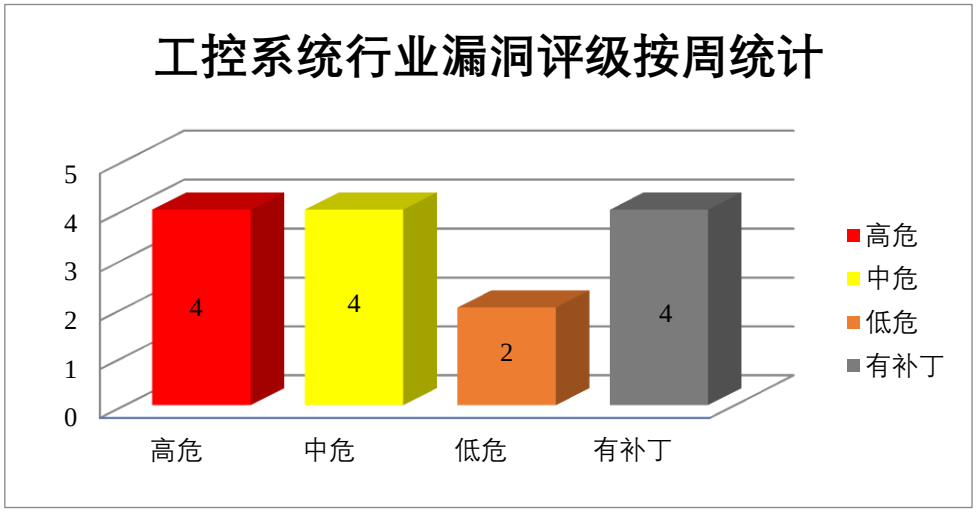

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft HEIF Image Extensions 是美国微软（Microsoft）公司的微软 Windows 系统得一个功能库。Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Paint 3D 是一款电脑画图软件，该软件在原有基础上做出了优化调整，并且加入了全新的、全面的画图工具，能够将平面的 2D 图像逐渐演变成 3D 图像。Microsoft Windows ALPC 是美国微软（Microsoft）公司发展出来替代 LPC，用于本机 RPC 的一种 C/S 模型技术。Microsoft Windows 是美国微软（Microsoft）公司的一个光盘驱动器。Microsoft Windows Cloud Files Mini Filter Driver 是美国微软（Microsoft）公司的一款云文件过滤器驱

动程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft HEIF Image Extensions 远程代码执行漏洞、Microsoft Office Visio 远程代码执行漏洞（CNVD-2022-77995、CNVD-2022-77996）、Microsoft Paint 3D 远程代码执行漏洞、Microsoft Windows ALPC 权限提升漏洞（CNVD-2022-78027、CNVD-2022-78053）、MIcrosoft Windows CD-ROM Driver 权限提升漏洞、Microsoft Windows Cloud Files Mini Filter Driver 权限提升漏洞。其中，“MIcrosoft Windows CD-ROM Driver 权限提升漏洞” 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-2022-77994
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77995
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77996
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78026
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78027
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78053
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78075
https://www.cnvd.org.cn/flaw/show/CNVD-2022-78155

2、F5 产品安全漏洞

F5 BIG-IP APM Edge Client for Windows 是 F5 公司的一款客户端访问控制认证接入客户端应用程序。F5 BIG-IP 是 F5 公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获得权限升级，在当前登录用户的上下文中执行 JavaScript，导致拒绝服务。

CNVD 收录的相关漏洞包括：F5 BIG-IP 代码问题漏洞（CNVD-2022-77521、CNVD-2022-77525）、F5 BIG-IP 输入验证错误漏洞（CNVD-2022-77524）、F5 BIG-IP 资源管理错误漏洞（CNVD-2022-77522、CNVD-2022-77526、CNVD-2022-77530）、F5 BIG-IP APM 跨站脚本漏洞（CNVD-2022-77527）、F5 BIG-IP 跨站脚本漏洞（CNVD-2022-77529）。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-2022-77521
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77524
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77522
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77527
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77526

https://www.cnvd.org.cn/flaw/show/CNVD-2022-77525

https://www.cnvd.org.cn/flaw/show/CNVD-2022-77530

https://www.cnvd.org.cn/flaw/show/CNVD-2022-77529

3、 Adobe 产品安全漏洞

Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe In Copy 是美国 Adobe 公司的一款用于创作的文本编辑软件。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敏感信息，在系统上执行任意代码，或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Adobe InDesign 代码执行漏洞（CNVD-2022-76624、CNVD-2022-76625）、Adobe InCopy 内存错误引用漏洞、Adobe InCopy 越界写入漏洞（CNVD-2022-76627）、Adobe Illustrator 代码执行漏洞、Adobe Illustrator 越界读取漏洞（CNVD-2022-76631、CNVD-2022-76632、CNVD-2022-76633）。其中，除“Adobe Illustrator 越界读取漏洞（CNVD-2022-76631）”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-2022-76624

https://www.cnvd.org.cn/flaw/show/CNVD-2022-76625

https://www.cnvd.org.cn/flaw/show/CNVD-2022-76626

https://www.cnvd.org.cn/flaw/show/CNVD-2022-76627

https://www.cnvd.org.cn/flaw/show/CNVD-2022-76629

https://www.cnvd.org.cn/flaw/show/CNVD-2022-76631

https://www.cnvd.org.cn/flaw/show/CNVD-2022-76632

https://www.cnvd.org.cn/flaw/show/CNVD-2022-76633

4、 IBM 产品安全漏洞

IBM InfoSphere Information Server 是美国 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 Business Automation Workflow 是美国 IBM 公司的一套工作流程自动化解决方案。该产品主要用于工作流程管理、合规性管理，并具有工作流程可见性和可扩展等特点。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 Rational Change 是美国 IBM 公司的一种软件工具。为与软件开发相关的所有工件提供了软件配置管理功能，包括源代码，文档和图像以及最终构建的软件可执行文件和库。IBM Maximo Asset Management 是美国国际商业机器（IBM）公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。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身份验证，获取敏感信息，

在受害者当前使用的环境中执行脚本，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 拒绝服务漏洞、IBM Business Automation Workflow 信息泄露漏洞、IBM InfoSphere Information Server CSV 注入漏洞、IBM InfoSphere Information Server 跨站请求伪造漏洞、IBM Robotic Process Automation 授权问题漏洞（CNVD-2022-77512）、IBM Rational Change 跨站脚本漏洞（CNVD-2022-77517）、IBM InfoSphere Information Server XML 外部实体注入（XXE）漏洞、IBM Maximo Asset Management 身份验证错误漏洞。其中，除“IBM InfoSphere Information Server 拒绝服务漏洞、IBM Business Automation Workflow 信息泄露漏洞、IBM Rational Change 跨站脚本漏洞（CNVD-2022-77517）”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-2022-77508
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77511
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77514
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77513
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77512
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77517
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77516
https://www.cnvd.org.cn/flaw/show/CNVD-2022-77520

5、TYPO3 Matomo Integration 组件跨站脚本漏洞

TYPO3 是瑞士 TYPO3 协会的一套免费开源的内容管理系统（框架）（CMS/CMF）。Matomo 是 Matomo 团队的一套网站统计分析平台。该平台包括访客统计、Web 分析、图表生成和 SEO 优化等功能。本周，TYPO3 Matomo Integration 组件被披露存在跨站脚本漏洞。该漏洞源于 Matomo Integration 组件缺少对用户提供的数据和输出的数据校验过滤。攻击者可利用该漏洞在网站中注入 JavaScript 代码。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-2022-76977

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-2022-76630	Adobe Illustrator 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://helpx.adobe.com/security/products/illustrator/apsb22-26.html

CNVD-2022-77071	LuxSoft LuxCal Web Calendar cookie 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.luxsoft.eu/index.php?pge=dload
CNVD-2022-77758	YAPI SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/YMFE/yapi/commit/59bade3a8a43e7db077d38a4b0c7c584f30ddf8c
CNVD-2022-77823	Fidelis Network and Deception 命令注入漏洞（CNVD-2022-77823）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fidelissecurity.zendesk.com/hc/en-us/articles/6211730139411
CNVD-2022-77879	OpenMRS SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wiki.openmrs.org/display/docs/Reporting+Bugs
CNVD-2022-77881	Magnitude Simba Amazon Athena ODBC Driver 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：https://www.magnitude.com/support
CNVD-2022-78140	Huawei HarmonyOS 权限提升漏洞（CNVD-2022-78140）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202211-0000001440896653
CNVD-2022-78144	Cisco Firepower Threat Defense 资源管理错误漏洞（CNVD-2022-78144）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-mgmt-privesc-7GqR2th
CNVD-2022-78210	Google Chrome 资源管理错误漏洞（CNVD-2022-78210）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop.html
CNVD-2022-78521	Tenda AC1206 缓冲区溢出漏洞	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.tenda.com.cn/download/detail-2766.html

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在系统上执行任意代码。此外，F5 、Apache、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身份验证，获取敏感信息，在系统上执行任意代码，或导致应用

程序崩溃等。另外，TYPO3 Matomo Integration 组件被披露存在跨站脚本漏洞。攻击者可利用漏洞在网站中注入 JavaScript 代码。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、Tenda AX180 堆栈溢出漏洞

验证描述

Tenda AX1803 是中国腾达（Tenda）公司的一款双频千兆 WIFI6 路由器。

Tenda AX1803 存在堆栈溢出漏洞。该漏洞是由于 fromSetIpMacBind 函数的边界检查不当造成的。攻击者可利用该漏洞使缓冲区溢出并在系统上执行任意代码，或者导致拒绝服务。

验证信息

POC 链接：https://github.com/Darry-lang1/vuln/tree/main/Tenda/AX1803/4

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-78484

信息提供者

北京神州绿盟科技有限公司

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. F5 BIG-IP 和 BIG-IQ 设备中报告安全漏洞，现已修复

F5 BIG-IP 和 BIG-IQ 设备中已披露多个安全漏洞，如果成功利用这些漏洞，将完全危害受影响的系统。这些问题会影响 BIG-IP 版本 13.x、14.x、15.x、16.x 和 17.x 以及 BIG-IQ 集中管理版本 7.x 和 8.x。

参考链接：https://thehackernews.com/2022/11/high-severity-vulnerabilities-reported.html

2. Spotify 后台软件目录和开发者平台报告 RCE 漏洞

Spotify 的 Backstage 被发现容易受到安全漏洞的影响，该漏洞可以通过利用第三方模块中最近披露的漏洞来远程执行代码。

参考链接：https://thehackernews.com/2022/11/critical-rce-flaw-reported-in-spotifys.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