国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 09 月 26 日-2022 年 10 月 09 日 **2022 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 469 个，其中高危漏洞 151 个、中危漏洞 226 个、低危漏洞 92 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 238 个（占 51%），其中互联网上出现“GPAC 缓冲区溢出漏洞（CNVD-2022-66588）、ZZCMS index php 信息泄露漏洞”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 22950 个，与上周（27685 个）环比减少 17%。

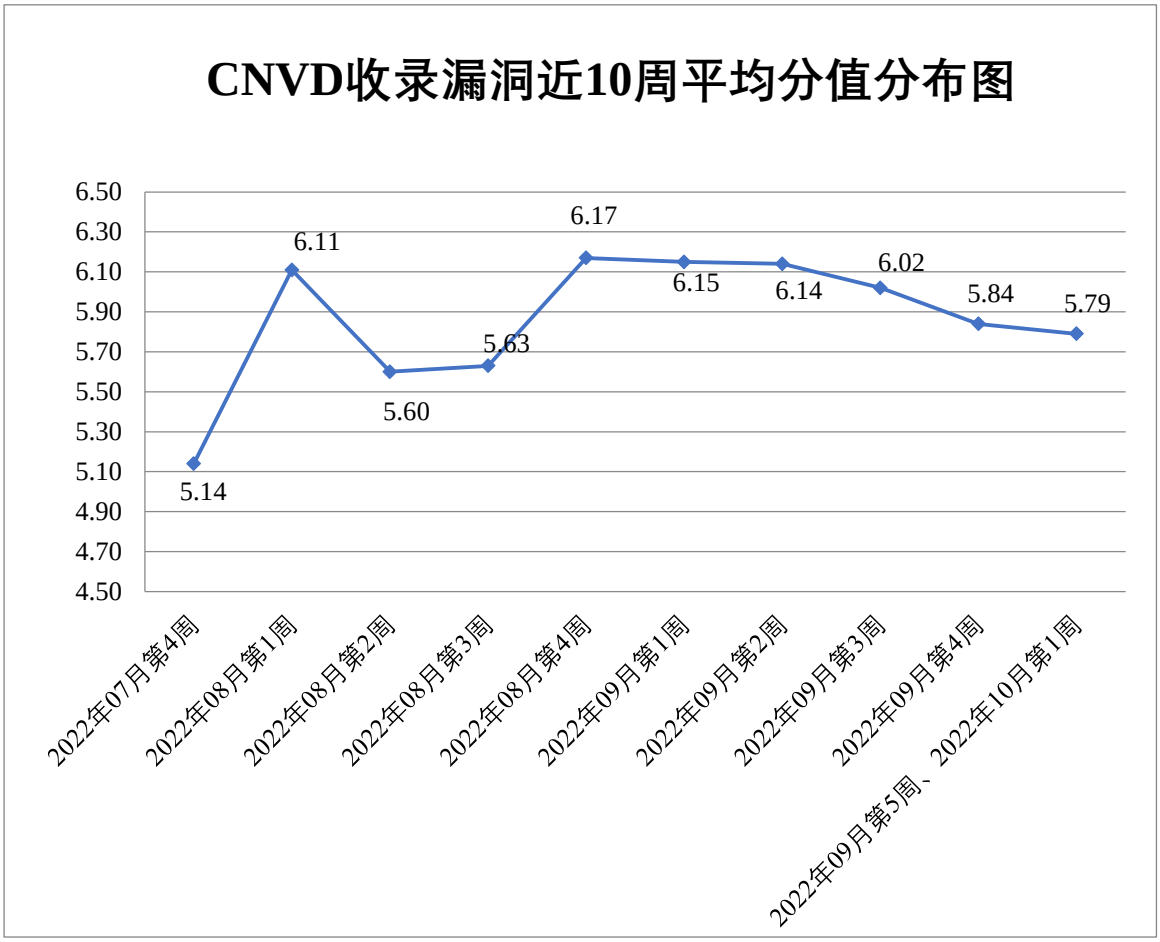

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 35 起，向基础电信企业通报漏洞事件 37 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 1082 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 222 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 130 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：

珠海格力电器股份有限公司、珠海高凌信息科技股份有限公司、重庆梅安森科技股份有限公司、智互联（深圳）科技有限公司、郑州安然测控技术股份有限公司、浙江浙大中控信息技术有限公司、浙江和达科技股份有限公司、浙江大华技术股份有限公司、运动秀（厦门）信息科技有限公司、云智慧（北京）科技有限公司、友讯电子设备（上海）有限公司、优酷信息技术（北京）有限公司、用友网络科技股份有限公司、宜昌三峡广播电视台、新金星软件服务（深圳）有限公司、心品网络科技有限公司、小米科技有限责任公司、西安众邦网络科技有限公司、西安新软信息科技有限公司、西安交大捷普网络科技有限公司、武汉思维跳跃科技有限公司、武汉达梦数据库股份有限公司、乌鲁木齐公共停车场服务管理有限公司、太原迅易科技有限公司、四川易简天下科技股份有限公司、四川品杰科技有限公司、石家庄市七星网络有限公司、神州数码集团股份有限公司、深圳维盟科技股份有限公司、深圳市亿图软件有限公司、深圳市迅雷网文化有限公司、深圳市网视无忧科技有限公司、深圳市腾讯计算机系统有限公司、深圳市思迅软件股份有限公司、深圳市蓝凌软件股份有限公司、深圳市金蝶天燕云计算股份有限公司、深圳市捷视飞通科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市福斯康姆智能科技有限公司、深圳市博思协创网络科技有限公司、深圳市必联电子有限公司、深圳齐心好视通云计算有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海优恒酒店管理有限公司、上海上业信息科技股份有限公司、上海商创网络科技有限公司、上海森栩医学科技有限公司、上海拉扎斯信息科技有限公司、上海凯京信达科技集团有限公司、上海孚盟软件有限公司、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、上海程江科技中心、上海布雷德科技有限公司、上海博达数据通信有限公司、上海贝锐信息科技股份有限公司、上海百酷信息科技有限公司、上海安达通信息安全技术股份有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山西企凝信息科技有限公司、山东潍微科技股份有限公司、山东金钟科技集团股份有限公司、厦门亿联网络技术股份有限公司、厦门四信通信科技有限公司、瑞斯康达科技发展股份

有限公司、青木数字技术股份有限公司、青岛东胜伟业软件科技有限公司、千城智联（上海）网络科技有限公司、千城云科（上海）数据科技有限公司、麒麟软件有限公司、普元电力发展有限公司、普联技术有限公司、南京物橙信息技术有限公司、纳龙科技有限公司、洛阳云业信息科技有限公司、联奕科技股份有限公司、联想（北京）有限公司、乐星电气（无锡）有限公司、快捷达通信设备（东莞）有限公司、精英数智科技股份有限公司、京信网络系统股份有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、江西金磊科技发展有限公司、江苏华御威盾网络科技有限公司、济南宇霞信息技术有限公司、吉翁电子（深圳）有限公司、黄石市科威自控有限公司、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、恒锋信息科技股份有限公司、河南易税科技有限公司、杭州雄伟科技开发股份有限公司、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、杭州恩软信息技术有限公司、国泰新点软件股份有限公司、广州市奥威亚电子科技有限公司、广州酷狗计算机科技有限公司、广州红帆科技有限公司、广州好象科技有限公司、广州佰能信息科技有限公司、广东泰恪网络科技有限公司、广东开太平信息科技有限责任公司、福州联讯信息科技有限公司、福建省华渔教育科技有限公司、福建榕基软件股份有限公司、福建福昕软件开发股份有限公司、大唐电信科技股份有限公司、大连华天软件有限公司、成都索贝数码科技股份有限公司、成都时空超越软件科技有限公司、畅捷通信息技术股份有限公司、北京中广上洋科技股份有限公司、北京致远互联软件股份有限公司、北京星网锐捷网络技术有限公司、北京星动次元网络科技有限公司、北京万户软件技术有限公司、北京通达志成科技有限公司、北京通达信科科技有限公司、北京天生创想信息技术有限公司、北京升鑫网络科技有限公司（青藤云）、北京神州视翰科技有限公司、北京上云科技发展有限公司、北京龙软科技股份有限公司、北京领雾科技有限公司、北京京东叁佰陆拾度电子商务有限公司、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、北京华宇信息技术有限公司、北京华医网科技股份有限公司、北京国尚信科技有限公司、北京倍胜智能科技有限公司、北京梆梆安全科技有限公司、北京百卓网络技术有限公司、北京爱语吧科技有限公司和安美世纪（北京）科技有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、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、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、南京众智维信息科技有限公司、西安四叶草信息技术有限公司、卫士通信息产业股份有限公司、内蒙古云科数据服务股份有限公司、中国电信股份有限公司网络安全产品运营中心、沈阳东软系统集成工程有限公司、北京华顺信安信息技术有限公司、山

东云天安全技术有限公司、河南信安世纪科技有限公司、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、北京山石网科信息技术有限公司、重庆都会信息科技有限公司、河南东方云盾信息技术有限公司、山石网科通信技术股份有限公司、杭州美创科技有限公司、苏州棱镜七彩信息科技有限公司、长春嘉诚信息技术股份有限公司、江西和尔惠信息技术有限公司、浙江木链物联网科技有限公司、山东新潮信息技术有限公司、福建省海峡信息技术有限公司、北京六方云信息技术有限公司、北京微步在线科技有限公司、北京升鑫网络科技有限公司、内蒙古信元网络安全技术股份有限公司、北京安帝科技有限公司、快页信息技术有限公司、平安银河实验室、上海纽盾科技股份有限公司、博智安全科技股份有限公司、成方金融科技有限公司上海分公司、浙江大学控制科学与工程学院、任子行网络技术股份有限公司、成都安美勤信息技术股份有限公司、广东唯顶信息科技股份有限公司、西安敏恒信息技术有限公司、中科华威（北京）信息技术研究院、浙江大华技术股份有限公司、联通沃悦读科技文化有限公司、福建浩程信息科技有限公司、国泰新点软件股份有限公司、北京快手科技有限公司、上海上讯信息技术股份有限公司、上海嘉韦思信息技术有限公司、北京君云天下科技有限公司、内蒙古中叶信息技术有限责任公司、上海安势信息技术有限公司、星云博创科技有限公司、江苏天竞云合数据技术有限公司、北京雪诺科技有限公司及其他个人白帽子向 CNVD 提交了 22950 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）、三六零数字安全科技集团有限公司、奇安信网神（补天平台）和上海交大向 CNVD 共享的白帽子报送的 20200 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）	11666	11666
三六零数字安全科技集团有限公司	3670	3670
奇安信网神（补天平台）	2937	2937
上海交大	1927	1927
深信服科技股份有限公司	533	0
新华三技术有限公司	404	0
远江盛邦（北京）网络安全科技股份有限公司	319	319
安天科技集团股份有限公司	307	3

北京神州绿盟科技有限公司	270	3
南京众智维信息科技有限公司	185	185
北京启明星辰信息安全技术有限公司	176	13
天津市国瑞数码安全系统股份有限公司	118	0
厦门服云信息科技有限公司	113	0
恒安嘉新（北京）科技股份公司	101	1
杭州安恒信息技术股份有限公司	96	55
北京天融信网络安全技术有限公司	91	8
北京数字观星科技有限公司	76	0
中国电信集团系统集成有限责任公司	55	0
西安四叶草信息技术有限公司	49	49
卫士通信息产业股份有限公司	47	47
内蒙古云科数据服务股份有限公司	19	19
沈阳东软系统集成工程有限公司	4	4
北京知道创宇信息技术股份有限公司	1	0
北京华顺信安信息技术有限公司	289	5
山东云天安全技术有限公司	72	72
河南信安世纪科技有	60	60

限公司		
奇安星城网络安全运营服务（长沙）有限公司	48	48
杭州默安科技有限公司	43	43
杭州迪普科技股份有限公司	21	0
北京山石网科信息技术有限公司	19	19
重庆都会信息科技有限公司	16	16
河南东方云盾信息技术有限公司	16	16
山石网科通信技术股份有限公司	14	14
杭州美创科技有限公司	12	12
苏州棱镜七彩信息科技有限公司	10	10
长春嘉诚信息技术股份有限公司	7	7
江西和尔惠信息技术有限公司	6	6
浙江木链物联网科技有限公司	6	6
山东新潮信息技术有限公司	6	6
中国电信股份有限公司网络安全产品运营中心	5	5
福建省海峡信息技术有限公司	5	5
北京六方云信息技术有限公司	5	5

北京微步在线科技有限公司	4	4
北京升鑫网络科技有限公司	4	4
内蒙古信元网络安全技术股份有限公司	4	4
北京安帝科技有限公司	4	4
快页信息技术有限公司	4	4
平安银河实验室	3	3
上海纽盾科技股份有限公司	3	3
博智安全科技股份有限公司	3	3
成方金融科技有限公司上海分公司	3	3
浙江大学控制科学与工程学院	3	3
任子行网络技术股份有限公司	2	2
成都安美勤信息技术股份有限公司	2	2
广东唯顶信息科技股份有限公司	2	2
西安敏恒信息技术有限公司	2	2
中科华威（北京）信息技术研究院	2	2
浙江大华技术股份有限公司	1	1
联通沃悦读科技文化有限公司	1	1
福建浩程信息科技有限公司	1	1

国泰新点软件股份有限公司	1	1
北京快手科技有限公司	1	1
上海上讯信息技术股份有限公司	1	1
上海嘉韦思信息技术有限公司	1	1
北京君云天下科技有限公司	1	1
内蒙古中叶信息技术有限责任公司	1	1
上海安势信息技术有限公司	1	1
星云博创科技有限公司	1	1
江苏天竞云合数据技术有限公司	1	1
北京雪诺科技有限公司	1	1
CNCERT 浙江分中心	7	7
CNCERT 贵州分中心	4	4
CNCERT 内蒙古分中心	4	4
CNCERT 宁夏分中心	2	2
CNCERT 四川分中心	1	1
个人	1613	1613
报送总计	25513	22950

本周漏洞按类型和厂商统计

本周，CNVD 收录了 469 个漏洞。WEB 应用 202 个，应用程序 143 个，网络设备（交换机、路由器等网络端设备）45 个，操作系统 42 个，智能设备（物联网终端设备）23 个，数据库 7 个，安全产品 7 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	202
应用程序	143
网络设备（交换机、路由器等网络端设备）	45
操作系统	42
智能设备（物联网终端设备）	23
数据库	7
安全产品	7

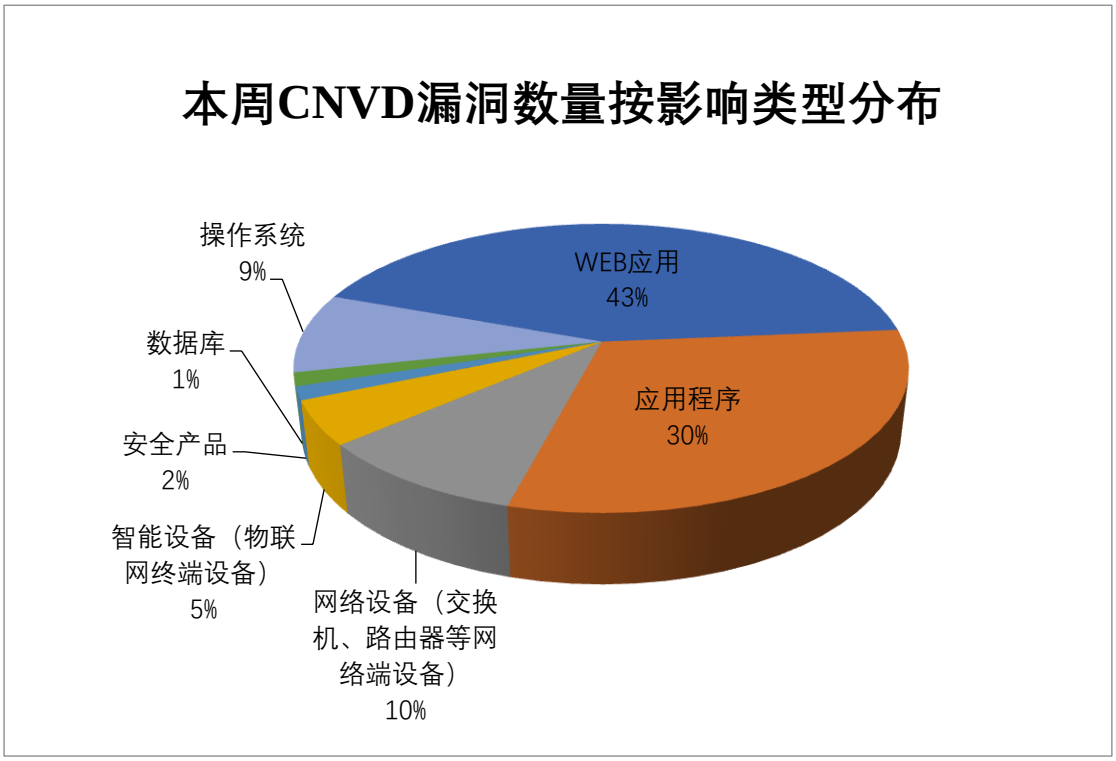

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Jenkins、IBM 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	39	8%
2	Jenkins	18	4%
3	IBM	15	3%
4	Google	14	3%
5	Microsoft	13	3%
6	Samsung	12	3%
7	Huawei	11	2%
8	Adobe	10	2%

9	MediaTek	9	2%
10	其他	328	70%

本周行业漏洞收录情况

本周，CNVD 收录了 43 个电信行业漏洞，34 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Google Android 代码执行漏洞（CNVD-2022-65629）、Bosch Ethernet switch PRA-ES8P2S Web 服务权限提升漏洞”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/

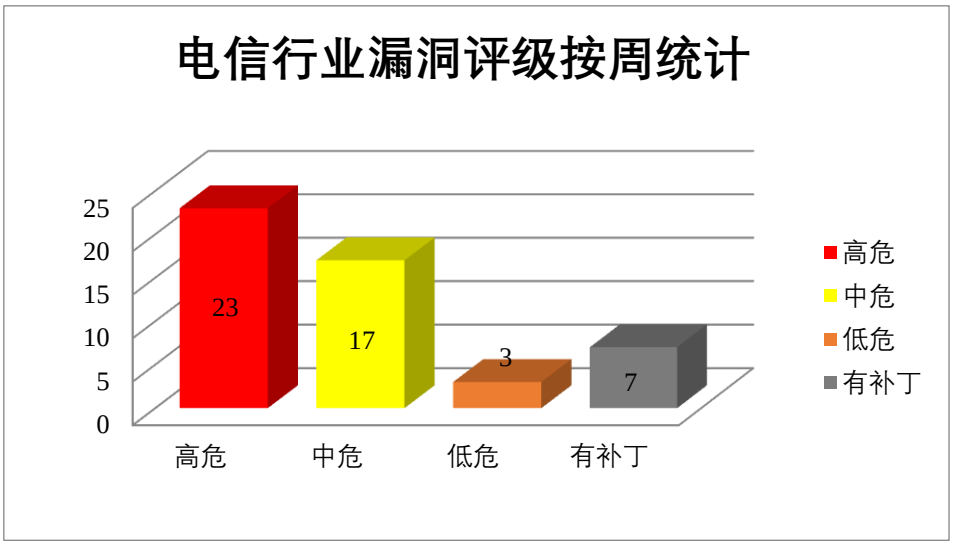

图 3 电信行业漏洞统计

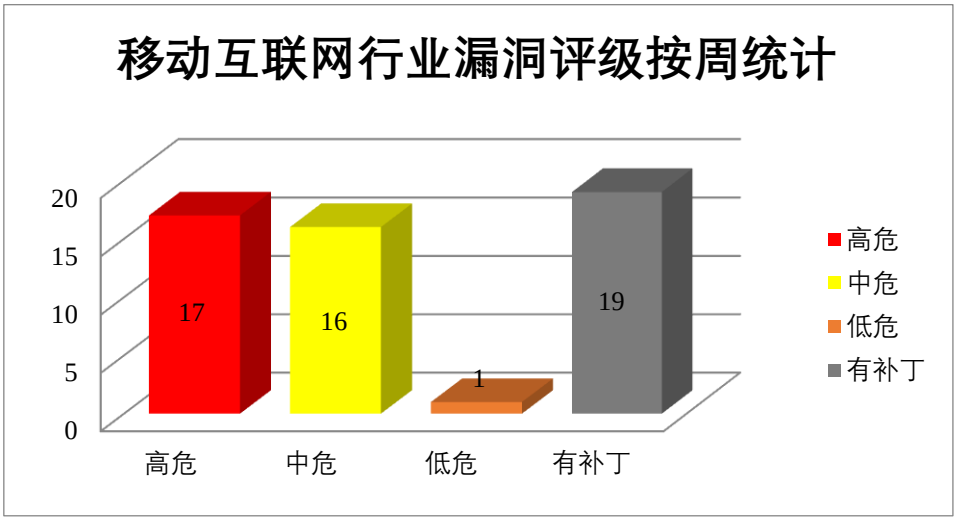

图 4 移动互联网行业漏洞统计

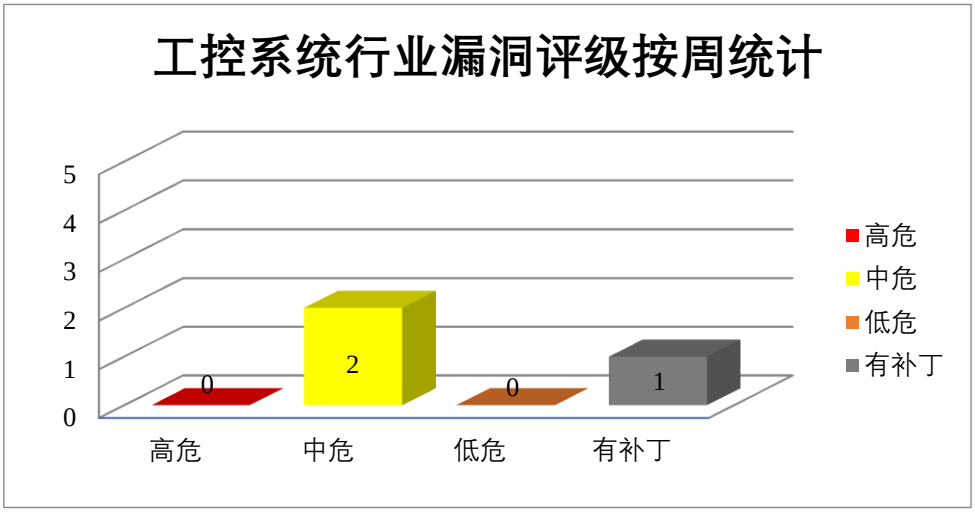

图 5 工控系统行业漏洞统计

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，攻击者可利用漏洞提升权限，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-65631、CNVD-2022-65633、CNVD-2022-65639、CNVD-2022-65636、CNVD-2022-65640、CNVD-2022-65641、CNVD-2022-65642）、Google Android 代码执行漏洞（CNVD-2022-65638）。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-2022-65631

https://www.cnvd.org.cn/flaw/show/CNVD-2022-65633

https://www.cnvd.org.cn/flaw/show/CNVD-2022-65639

https://www.cnvd.org.cn/flaw/show/CNVD-2022-65638

https://www.cnvd.org.cn/flaw/show/CNVD-2022-65636

https://www.cnvd.org.cn/flaw/show/CNVD-2022-65640

https://www.cnvd.org.cn/flaw/show/CNVD-2022-65641

https://www.cnvd.org.cn/flaw/show/CNVD-2022-65642

2、 Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。Microsoft Windows Kernel 是美国微软（Microsoft）公司的 Windows 操作系统的内核。

Microsoft Windows Installer 是美国微软（Microsoft）公司的 Windows 操作系统的一个组件。为安装和卸载软件提供了标准基础。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，导致权限提升，造成拒绝服务。

CNVD 收录的相关漏洞包括：Microsoft Windows Secure Channel 拒绝服务漏洞、Microsoft Windows Telephony Serve 权限提升漏洞、Microsoft Windows Upgrade Assistant 远程代码执行漏洞、Microsoft Windows Kernel 信息泄露漏洞（CNVD-2022-65612）、Microsoft Windows Digital Media Receiver 提升权限漏洞、Microsoft Windows Endpoint Configuration Manager 权限提升漏洞、Microsoft Windows Installer 权限提升漏洞、Microsoft Windows iSCSI Target Service 信息泄露漏洞。其中，“Microsoft Windows Telephony Serve 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-2022-65610
https://www.cnvd.org.cn/flaw/show/CNVD-2022-65609
https://www.cnvd.org.cn/flaw/show/CNVD-2022-65608
https://www.cnvd.org.cn/flaw/show/CNVD-2022-65612
https://www.cnvd.org.cn/flaw/show/CNVD-2022-65611
https://www.cnvd.org.cn/flaw/show/CNVD-2022-65616
https://www.cnvd.org.cn/flaw/show/CNVD-2022-65615
https://www.cnvd.org.cn/flaw/show/CNVD-2022-65614

3、Adobe 产品安全漏洞

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe Photoshop 是一个由 Adobe 公司开发和发行的应用软件，用于图像处理。Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。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任意文件，在当前用户的上下文中执行任意代码，导致缓冲区溢出等。

CNVD 收录的相关漏洞包括：Adobe Bridge 资源管理错误漏洞（CNVD-2022-66014、CNVD-2022-66013）、Adobe Photoshop 缓冲区溢出漏洞（CNVD-2022-66018、CNVD-2022-66021、CNVD-2022-66022）、Adobe InDesign 缓冲区溢出漏洞（CNVD-2022-66017）、Adobe Bridge 缓冲区溢出漏洞（CNVD-2022-66015）、Adobe Experience Manager 跨站脚本漏洞（CNVD-2022-66019）。其中，除“Adobe Bridge 资源管理错误漏洞（CNVD-2022-66014）、Adobe InDesign 缓冲区溢出漏洞（CNVD-2022-66017）、Adobe Experience Manager 跨站脚本漏洞（CNVD-2022-66019）”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-2022-66014

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66013

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66018

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66017

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66015

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66019

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66021

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66022

4、IBM 产品安全漏洞

IBM Security Identity Governance and Intelligence（IGI）是美国 IBM 公司的一套身份治理解决方案。该产品包括生命周期管理、访问风险评估和身份认证管理等功能。IBM Cognos Controller 是美国 IBM 公司的一套商业智能与计划解决方案。该产品具有流程自动化、财务审计控制、创建和管理财务报告等功能。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 Guardium Data Encryption 是获取定价信息、用于保护数据和业务的加密解决方案 。IBM Engineering Requirements Quality Assistant 是美国 IBM 公司的一款基于 Watson AI 用于辅助开发人员提高工程需求质量的软件。该应用可显著降低发现缺陷成本，有利于尽早发现工程流程中的需求错误，加快产品上市。IBM Data Virtualization on Cloud Pak for Data 是美国 IBM 公司的一种云原生解决方案。可让您快速高效地使用数据。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。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或消耗内存资源，在 Web UI 中嵌入任意 JavaScript 代码，造成应用拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Security Identity Governance and Intelligence 信息泄露漏洞（CNVD-2022-66259）、IBM Cognos Controller XML 外部实体注入漏洞（CNVD-2022-66264、CNVD-2022-66265）、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-2022-66262）、IBM Guardium Data Encryption 信息泄漏漏洞（CNVD-2022-66261）、IBM Engineering Requirements Quality Assistant 拒绝服务漏洞、IBM Data Virtualization on Cloud Pak for Data 信息泄露漏洞、IBM Business Automation Workflow 和 Business Process Manager 信息泄露漏洞。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-2022-66259

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66264

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66262

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66261

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66266

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66265

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66268

https://www.cnvd.org.cn/flaw/show/CNVD-2022-66267

5、Linux kernel 拒绝服务漏洞（CNVD-2022-66585）

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，Linux kernel 被披露存在拒绝服务漏洞。攻击者可利用该漏洞通过 io_uring 触发 Linux kernel 的内存损坏，从而导致拒绝服务。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-2022-66585

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：https://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-2022-65630	Google Android 代码执行漏洞（CNVD-2022-65630）	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://source.android.com/security/bulletin/pixel/2022-08-01
CNVD-2022-66183	Huawei HarmonyOS 缓冲区溢出漏洞（CNVD-2022-66183）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202201-0000001238736331
CNVD-2022-66404	VoIPmonitor SQL 注入漏洞（CNVD-2022-66404）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.voipmonitor.org/changelog-gui?major=5
CNVD-2022-66621	WordPress MOLIE plugin 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://wpscan.com/vulnerability/cf907d53-cc4a-4b02-bed3-64754128112c
CNVD-2022-66671	Pillow 缓冲区溢出漏洞（CNVD-2022-66671）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/python-pillow/Pillow/releases/tag/9.1.1
CNVD-2022-66692	GPAC 内存错误引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/gpac/gpac/commit

			/c535bad50d5812d27ee5b22b54371bddec411514
CNVD-2022-66691	Bludit 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/bludit/bludit/issues/1242
CNVD-2022-66763	Vim 缓冲区溢出漏洞（CNVD-2022-66763）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/vim/vim/commit/8279af514ca7e5fd3c31cf13b0864163d1a0bfeb
CNVD-2022-66770	Centreon SQL 注入漏洞（CNVD-2022-66770）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/centreon/centreon/releases/tag/22.04.1
CNVD-2022-65635	Google Android 拒绝服务漏洞（CNVD-2022-65635）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source..com/security/bulletin/2022-08-01

小结：本周，Google 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，Microsoft、Adobe、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件，获取敏感信息，执行任意代码，导致权限提升，造成拒绝服务等。另外，Linux kernel 被披露存在拒绝服务漏洞。攻击者可利用该漏洞通过 io_uring 触发 Linux kernel 的内存损坏，从而导致拒绝服务。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、GPAC 缓冲区溢出漏洞（CNVD-2022-66588）

验证描述

GPAC 是一款开源的多媒体框架。

GPAC 2.0.0 存在缓冲区溢出漏洞，该漏洞源于滥用 utils/utf.c 中的 Unicode utf8_wcslen(改名为 gf_utf8_wcslen)函数，攻击者可利用该漏洞导致基于堆的缓冲区过读。

验证信息

POC 链接：https://github.com/gpac/gpac/files/8555402/POC.zip

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-66588

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. WhatsApp 漏洞可能让攻击者远程入侵设备

WhatsApp 已发布安全更新，以解决其 Android 和 iOS 消息应用程序中的两个缺陷，这些缺陷可能导致在易受攻击的设备上远程执行代码。

参考链接：https://thehackernews.com/2022/09/critical-whatsapp-bugs-could-have-let.html

2. CVE-2022-30331-TigerGraph 3.6.0 UDF 功能漏洞分析

TigerGraph 图数据库为用户提供了远程上传任意 C++源代码以创建用户定义函数的工具。该代码会自动编译并安装到敏感的系统组件中，几乎不需要仔细检查。由于缺乏保护措施，这个过程可以以最小的权限被利用，让攻击者完全控制整个 TigerGraph 集群和底层服务器。

参考链接：https://www.freebuf.com/vuls/345066.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