国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 05 月 29 日-2023 年 06 月 04 日 **2023 年第 22 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 370 个，其中高危漏洞 163 个、中危漏洞 164 个、低危漏洞 43 个。漏洞平均分值为 6.45。本周收录的漏洞中，涉及 0day 漏洞 278 个（占 75%），其中互联网上出现“Bludit 跨站脚本漏洞（CNVD-2023-43230）、nopCommerce 访问控制错误漏洞”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 12598 个，与上周（6973 个）环比增加 81%。

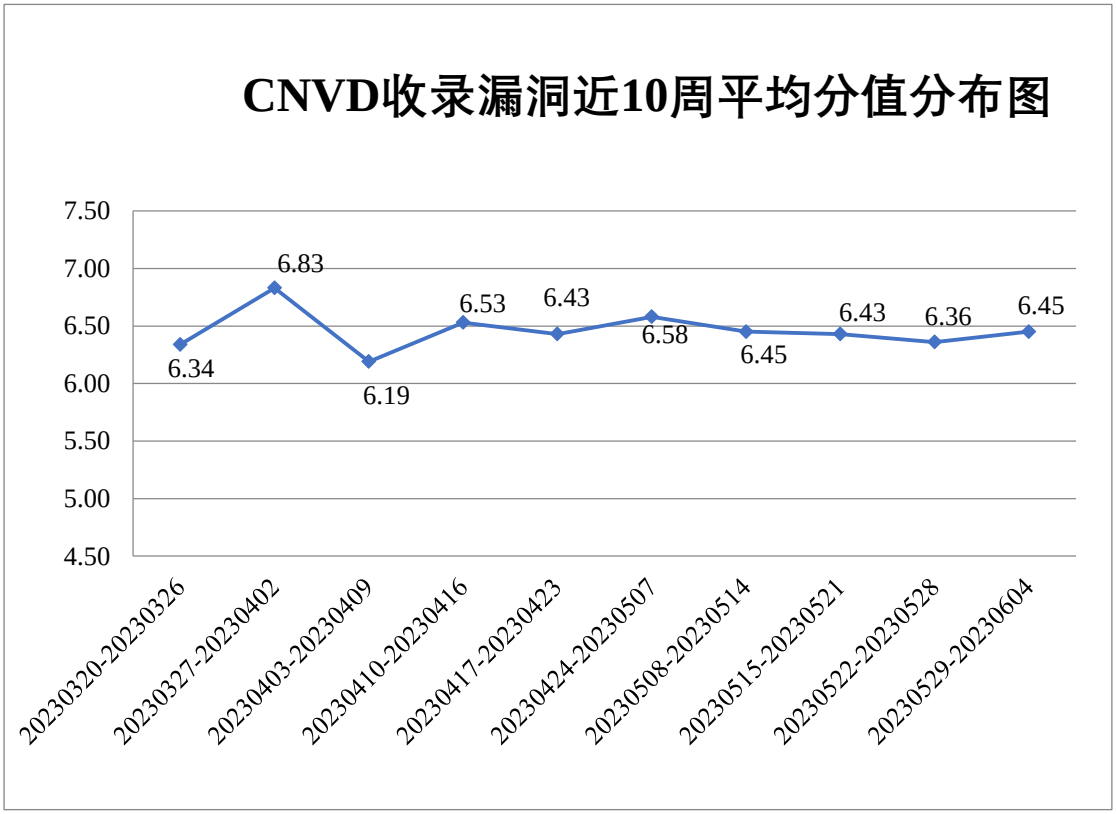

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 26 起，向基础电信企业通报漏洞事件 33 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 1060 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 157 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 56 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：

重庆啄木鸟网络科技有限公司、重庆悠度科技有限公司、重庆冰炫科技有限公司、浙江码尚科技股份有限公司、浙江兰德纵横网络技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技有限公司、研华科技（中国）有限公司、新天科技股份有限公司、新励成教育科技股份有限公司、万洲电气股份有限公司、万兴科技集团股份有限公司、同方健康科技（北京）股份有限公司、天闻数媒科技(北京)有限公司、天津鸿软通联信息技术有限公司、宿州市涛盛网络科技有限公司、圣原健康产业有限公司、深圳市英威腾电气股份有限公司、深圳市伟博思技术有限公司、深圳市捷视飞通科技股份有限公司、深圳市捷道智控实业有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市必联电子有限公司、深圳市昂捷信息技术股份有限公司、深圳科士达科技股份有限公司、深圳博阳好易信息技术有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海中通快递股份有限公司、上海易正信息技术有限公司、上海鑫谊麟禾科技有限公司、上海商派网络科技有限公司、上海穆云智能科技有限公司、上海米健信息技术有限公司、上海寰创通信科技股份有限公司、厦门四信通信科技有限公司、厦门纳龙健康科技股份有限公司、厦门科拓通讯技术股份有限公司、朴和教育科技有限公司、鹏为软件股份有限公司、迈普通信技术股份有限公司、力合科技（湖南）股份有限公司、理光（中国）投资有限公司、昆明珍茗食品有限责任公司、京瓷办公信息系统株式会社、金蝶软件（中国）有限公司、江西铭软科技有限公司、佳之易网络有限公司、佳能（中国）有限公司、济南驰骋信息技术有限公司、惠普贸易（上海）有限公司、湖南强智科技发展有限公司、河南迈亿电子商务有限公司、杭州中智游文旅科技有限公司、杭州中沛电子有限公司、杭州联科美讯生物医药技术有限公司、杭州飞致云信息科技有限公司、哈尔滨伟成科技有限公司、桂林市利通电子科技有限责任公司、贵阳朗玛信息技术股份有限公司、广州中海达卫星导航技术股份有限公司、广州市九二网络科技有限公司、广州市国万电子科技有限公司、广州牧云网络科技有限公司、广州铭莱信息科技有限公司、广州红帆科技有限公司、东莞市宇腾信息科技有限公司、东莞市冬惊鱼网络科技有限公司、帝国软件、成都市国卫信安信息技术有限公司、成都零起飞科技有限公司、贝尔金国际有限公司、北京竹间科技有限公司、北京中农信达信

息技术有限公司、北京易普拉格科技股份有限公司、北京维网云数据科技有限公司、北京网御星云信息技术有限公司、北京万讯博通科技发展有限公司、北京通达信科科技有限公司、北京神州数码云科信息技术有限公司、北京力控元通科技有限公司、北京兰云科技有限公司、北京金盘鹏图软件技术有限公司、北京国尚信科技有限公司、北京东方通科技股份有限公司、北京百卓网络技术有限公司、保定远信软件科技有限公司、巴可伟视（北京）电子有限公司、安美世纪（北京）科技有限公司、安徽阳光心健科技发展有限公司、ZZCMS、yycms、semcms、PHPMyWind、NETGEAR、kkcms、jeewms 和 Catfish CMS。

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、新华三技术有限公司、深信服科技股份有限公司、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。快页信息技术有限公司、上海齐同信息科技有限公司、河南东方云盾信息技术有限公司、中孚安全技术有限公司、内蒙古洞明科技有限公司、杭州默安科技有限公司、河南信安世纪科技有限公司、杭州美创科技有限公司、贵州多彩网安科技有限公司、联想集团、中国电信股份有限公司上海研究院、重庆电信系统集成公司、成都思维世纪科技有限责任公司、宁夏凯信特信息科技有限公司、北京山石网科信息技术有限公司、广州安亿信软件科技有限公司、赛尔网络有限公司、中国工商银行股份有限公司软件开发中心、河南省鼎信信息安全等级测评有限公司、河北锎远网络科技有限公司、郑州埃文科技、江苏天竞云合数据技术有限公司、信联科技（南京）有限公司、软通动力信息技术（集团）股份有限公司、北京珞安科技有限责任公司、重庆易阅科技有限公司、平安银河实验室、上海嘉韦思信息技术有限公司、黑龙江亿林网络股份有限公司及其他个人白帽子向 CNVD 提交了 12598 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 10679 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）	7125	7125
奇安信网神（补天平台）	2488	2488
三六零数字安全科技集团有限公司	774	774
北京启明星辰信息安	696	1

全技术有限公司		
新华三技术有限公司	457	0
深信服科技股份有限公司	312	7
上海交大	292	292
安天科技集团股份有限公司	240	0
北京神州绿盟科技有限公司	231	2
北京数字观星科技有限公司	199	0
阿里云计算有限公司	180	1
北京天融信网络安全技术有限公司	151	2
北京长亭科技有限公司	123	0
南京众智维信息科技有限公司	102	102
天津市国瑞数码安全系统股份有限公司	59	0
京东科技信息技术有限公司	45	6
中国电信集团系统集成有限责任公司	32	9
北京安信天行科技有限公司	22	22
杭州迪普科技股份有限公司	14	0
远江盛邦（北京）网络安全科技股份有限公司	10	10
卫士通信息产业股份有限公司	9	9
北京知道创宇信息技术有限公司	4	2

北京智游网安科技有限公司	2	2
浙江大华技术股份有限公司	1	1
杭州安恒信息技术股份有限公司	1	1
快页信息技术有限公司	287	287
上海齐同信息科技有限公司	146	146
河南东方云盾信息技术有限公司	71	71
中孚安全技术有限公司	49	49
内蒙古洞明科技有限公司	44	44
杭州默安科技有限公司	24	24
河南信安世纪科技有限公司	16	16
杭州美创科技有限公司	13	13
贵州多彩网安科技有限公司	13	13
联想集团	12	12
中国电信股份有限公司上海研究院	9	9
重庆电信系统集成公司	9	9
成都思维世纪科技有限责任公司	6	6
宁夏凯信特信息科技有限公司	4	4
北京山石网科信息技术有限公司	4	4

广州安亿信软件科技有限公司	4	4
赛尔网络有限公司	4	4
中国工商银行股份有限公司软件开发中心	3	3
河南省鼎信信息安全等级测评有限公司	3	3
河北锐远网络科技有限公司	2	2
郑州埃文科技	2	2
江苏天竞云合数据技术有限公司	2	2
信联科技（南京）有限公司	1	1
软通动力信息技术（集团）股份有限公司	1	1
北京珞安科技有限责任公司	1	1
重庆易阅科技有限公司	1	1
平安银河实验室	1	1
上海嘉韦思信息技术有限公司	1	1
黑龙江亿林网络股份有限公司	1	1
CNCERT 贵州分中心	3	3
CNCERT 陕西分中心	2	2
个人	1003	1003
报送总计	15311	12598

本周漏洞按类型和厂商统计

本周，CNVD 收录了 370 个漏洞。WEB 应用 187 个，应用程序 111 个，网络设备（交换机、路由器等网络端设备）33 个，安全产品 22 个，操作系统 12 个，智能设备（物

联网终端设备）5 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	187
应用程序	111
网络设备（交换机、路由器等网络端设备）	33
安全产品	22
操作系统	12
智能设备（物联网终端设备）	5

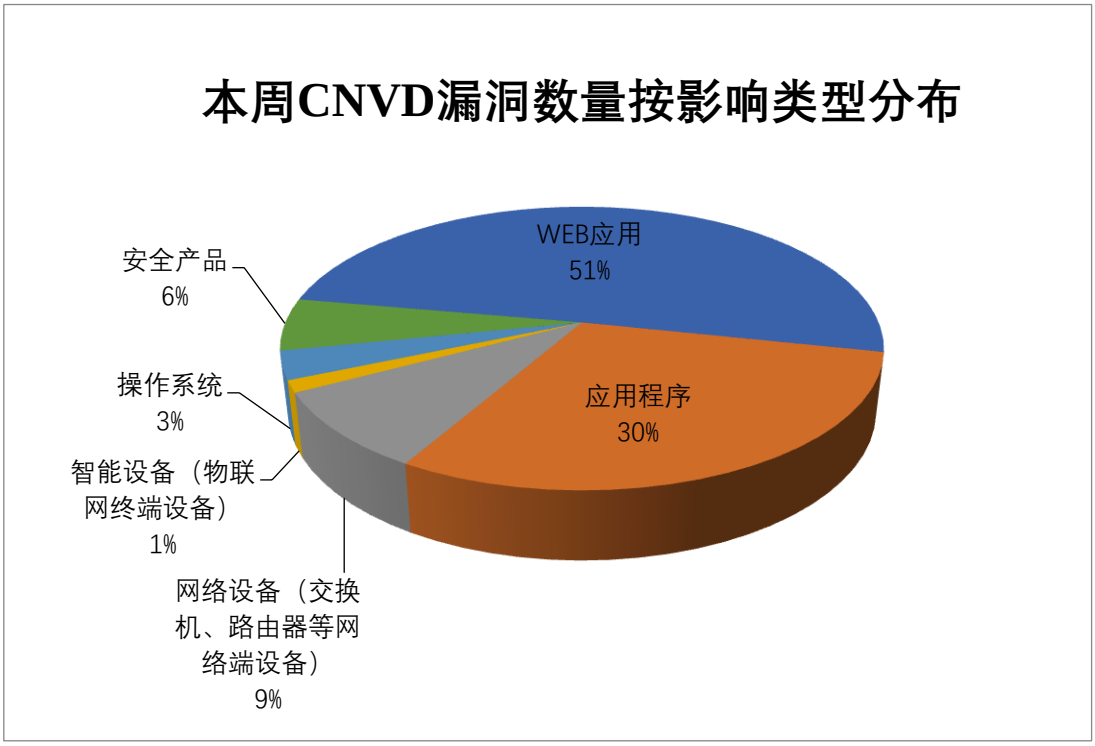

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apache、NETGEAR、北京通达信科科技有限公司等多家厂商的产品，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	Apache	24	6%
2	NETGEAR	17	5%
3	北京通达信科科技有限公司	14	4%
4	Google	13	4%
5	IBM	12	3%
6	Adobe	12	3%
9	新华三技术有限公司	8	2%

7	Dell	7	2%
8	JerryScript	6	2%
10	其他	257	69%

本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，38 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，“Google Android 权限提升漏洞（CNVD-2023-41877）、Schneider Electric IGSS Data Server alarm data 缓冲区溢出漏洞”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/

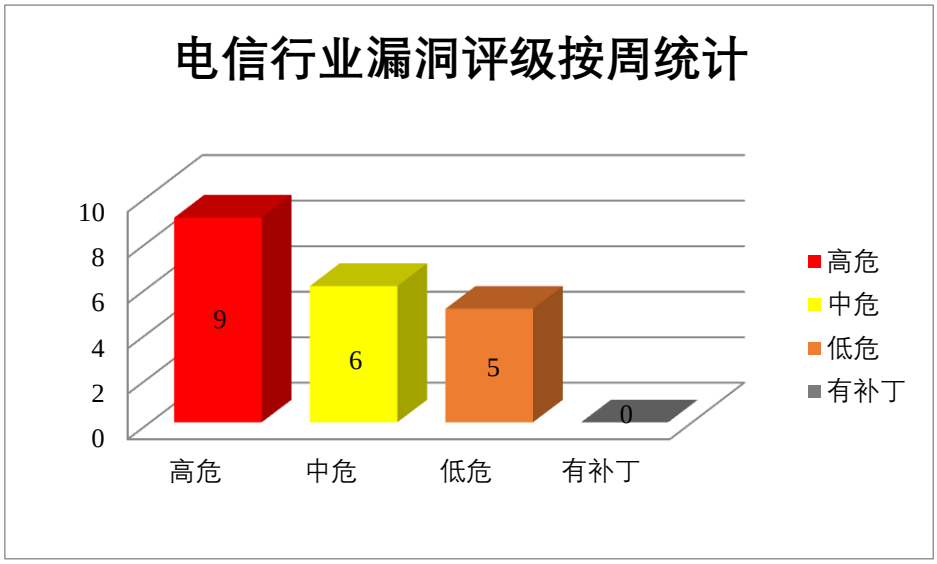

图 3 电信行业漏洞统计

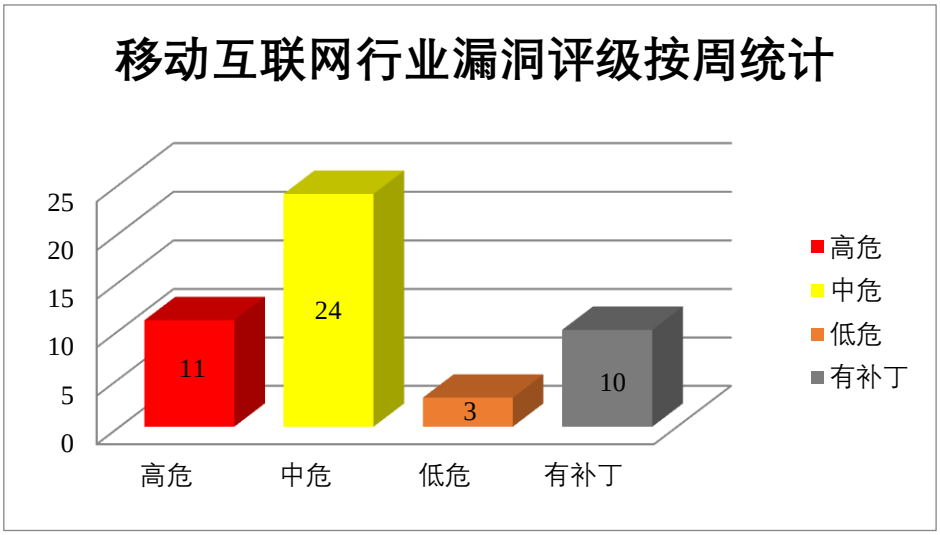

图 4 移动互联网行业漏洞统计

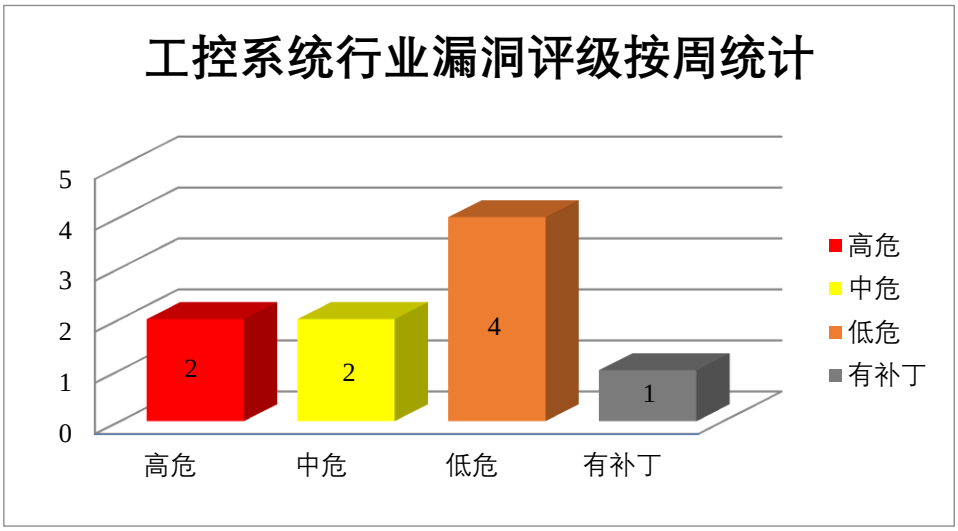

图 5 工控系统行业漏洞统计

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。Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面潜在地利用堆损坏，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-2023-41877、CNVD-2023-41878、CNVD-2023-41879、CNVD-2023-41881、CNVD-2023-41886）、Google Chrome Autofill UI 内存错误引用漏洞、Google Chrome Guest View 内存错误引用漏洞、Google Chrome DevTools 内存错误引用漏洞（CNVD-2023-43874）。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-2023-41877

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41878

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41879

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41881

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41886

https://www.cnvd.org.cn/flaw/show/CNVD-2023-43873

https://www.cnvd.org.cn/flaw/show/CNVD-2023-43875

https://www.cnvd.org.cn/flaw/show/CNVD-2023-43874

2、IBM 产品安全漏洞

IBM Cognos Analytics 是美国国际商业机器（IBM）公司的一套商业智能软件。该软件包括报表、仪表板和记分卡等，并可通过分析关键因素与关键人等内容，协助企业调整决策。IBM InfoSphere Information Server 是一款领先的集成平台，其服务产品可帮助您理解、清理、监控、转换和交付数据。IBM Spectrum Protect Plus 是美国国际商业机器（IBM）公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。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。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，攻击者可利用漏洞读取凭证，在 Web UI 中嵌入任意 JavaScript 代码，从而导致凭据泄露，执行任意代码，获取主机权限等。

CNVD 收录的相关漏洞包括：IBM Cognos Analytics 跨站脚本漏洞（CNVD-2023-41887）、IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2023-41891）、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-2023-41890）、IBM InfoSphere Information Server SQL 注入漏洞（CNVD-2023-41889）、IBM InfoSphere Information Server 代码执行漏洞、IBM Spectrum Protect Plus 信息泄露漏洞（CNVD-2023-41895）、IBM Security Verify Access 输入验证错误漏洞（CNVD-2023-41894）、IBM Planning Analytics 跨站脚本漏洞（CNVD-2023-41893）。其中，“IBM InfoSphere Information Server 代码执行漏洞、IBM Security Verify Access 输入验证错误漏洞（CNVD-2023-41894）”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-2023-41887
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41891
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41890
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41889
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41888
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41895
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41894
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41893

3、Apache 产品安全漏洞

Apache InLong 是美国阿帕奇（Apache）基金会的一站式的海量数据集成框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞删除、编辑、停止和启动他人的源，在系统上执行任意代码，提升权限等。

CNVD 收录的相关漏洞包括：Apache InLong 安全绕过漏洞（CNVD-2023-42958、CNVD-2023-42959、CNVD-2023-42962、CNVD-2023-42961）、Apache InLong 权限提

升漏洞、Apache InLong 安全绕过漏洞、Apache InLong 代码执行漏洞、Apache InLong 授权问题漏洞。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-2023-42958
https://www.cnvd.org.cn/flaw/show/CNVD-2023-42959
https://www.cnvd.org.cn/flaw/show/CNVD-2023-42962
https://www.cnvd.org.cn/flaw/show/CNVD-2023-42961
https://www.cnvd.org.cn/flaw/show/CNVD-2023-42963
https://www.cnvd.org.cn/flaw/show/CNVD-2023-42966
https://www.cnvd.org.cn/flaw/show/CNVD-2023-42965
https://www.cnvd.org.cn/flaw/show/CNVD-2023-42967

4、 Adobe 产品安全漏洞

Adobe Substance 3D Stager 是美国奥多比（Adobe）公司的一个虚拟 3D 工作室。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内存泄露，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 Substance 3D Stager 输入验证错误漏洞、Adobe Substance 3D Stager 越界读取漏洞（CNVD-2023-41873、CNVD-2023-41872、CNVD-2023-41875、CNVD-2023-41874）、Adobe Substance 3D Stager 资源管理错误漏洞（CNVD-2023-41871、CNVD-2023-41870）、Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2023-41876）。其中，“Adobe Substance 3D Stager 输入验证错误漏洞、Adobe Substance 3D Stager 资源管理错误漏洞（CNVD-2023-41871、CNVD-2023-41870）、Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2023-41876）”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-2023-41870
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41869
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41873
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41872
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41871
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41876
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41875
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41874

5、Tenda AC15 sub_E2F4 函数缓冲区溢出漏洞

Tenda AC15 是中国腾达（Tenda）公司的一款无线路由器。本周，Tenda AC15 被披露存在缓冲区溢出漏洞。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。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-2023-43044

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-2023-41897	IBM Cloud Pak for Data 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://www.ibm.com/support/pages/node/6980959
CNVD-2023-41896	IBM WebSphere Application Server 实体注入漏洞（CNVD-2023-41896）	高	厂商已发布了漏洞修复程序，请及时关注更新:https://exchange.xforce.ibmcloud.com/vulnerabilities/249185
CNVD-2023-42970	Apache Tomcat 拒绝服务漏洞（CNVD-2023-42970）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/7wvxonzwb7k9hx9jt3q33cmy7j97jo3j
CNVD-2023-42971	Apache RocketMQ 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp
CNVD-2023-42973	Apache OpenMeetings 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/j2d6mg3rzcphfd8vvvk09d8p4o9lvnqp
CNVD-2023-42974	Apache OpenMeetings 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://lists.apache.org/thread/230plvhbdx26m43b0sy942wlwt6kkmmr
CNVD-2023-43229	Rocket.Chat 授权问题漏洞（CNVD-2023-43229）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.rocket.chat/
CNVD-2023-43232	LibRaw 缓冲区溢出漏洞（CNVD-2023-43232）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/LibRaw/LibRaw/commit/9ab70f6dca19229cb5caad7cc31af4e7501bac93
CNVD-2023-43239	Dell EMC ECS 加密问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.dell.com/support/kbdoc/en-us/000212970/dsa-2023-109-dell-ecs-security-update-for-multiple-vulnerabilities
CNVD-2023-43249	Foxit PDF Reader and PDF Editor 越界读取漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxitsoftware.com/support/security-bulletins.php

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面潜在地利用堆损坏，获得提升的权限。此外，IBM、Apache、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞读取凭证，在 Web UI 中嵌入任意 JavaScript 代码，从而导致凭据泄露，执行任意代码，获取主机权限等。另外，Tenda AC15 被披露存在缓冲区溢出漏洞。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。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、Bludit 跨站脚本漏洞（CNVD-2023-43230）

验证描述

Bludit 是一套开源的轻量级博客内容管理系统（CMS）。

Bludit v3.14.1 版本存在跨站脚本漏洞。该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞可以通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://packetstormsecurity.com/files/172462/Bludit-CMS-3.14.1-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-43230

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. 招聘平台 Prosperix 泄漏求职者敏感信息

美国加州一家“劳动力创新”公司 Prosperix 泄漏了近 25 万份文件，部分文件中包含大量求职者的个人敏感数据。

参考链接：https://securityaffairs.com/146935/security/prosperix-data-leak.html

2. 6 月 1 日起，谷歌对 Chrome 的沙盒逃逸漏洞的奖金增加三倍

谷歌 6 月 1 日宣布，对其 Chrome 网络浏览器的沙盒逃逸链漏洞的奖励增加三倍，直至 2023 年 12 月 1 日。

参考链接：https://www.bleepingcomputer.com/news/google/google-triples-rewards-for-chrome-sandbox-escape-chain-exploits/

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