国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 12 月 04 日-2023 年 12 月 10 日 **2023 年第 49 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 531 个，其中高危漏洞 237 个、中危漏洞 257 个、低危漏洞 37 个。漏洞平均分值为 6.26。本周收录的漏洞中，涉及 0day 漏洞 449 个（占 85%），其中互联网上出现“PortlandLabs Concrete CMS 自定义标签字段跨站脚本漏洞、Dreamer CMS 跨站请求伪造漏洞”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 22289 个，与上周（19630 个）环比增加 14%。

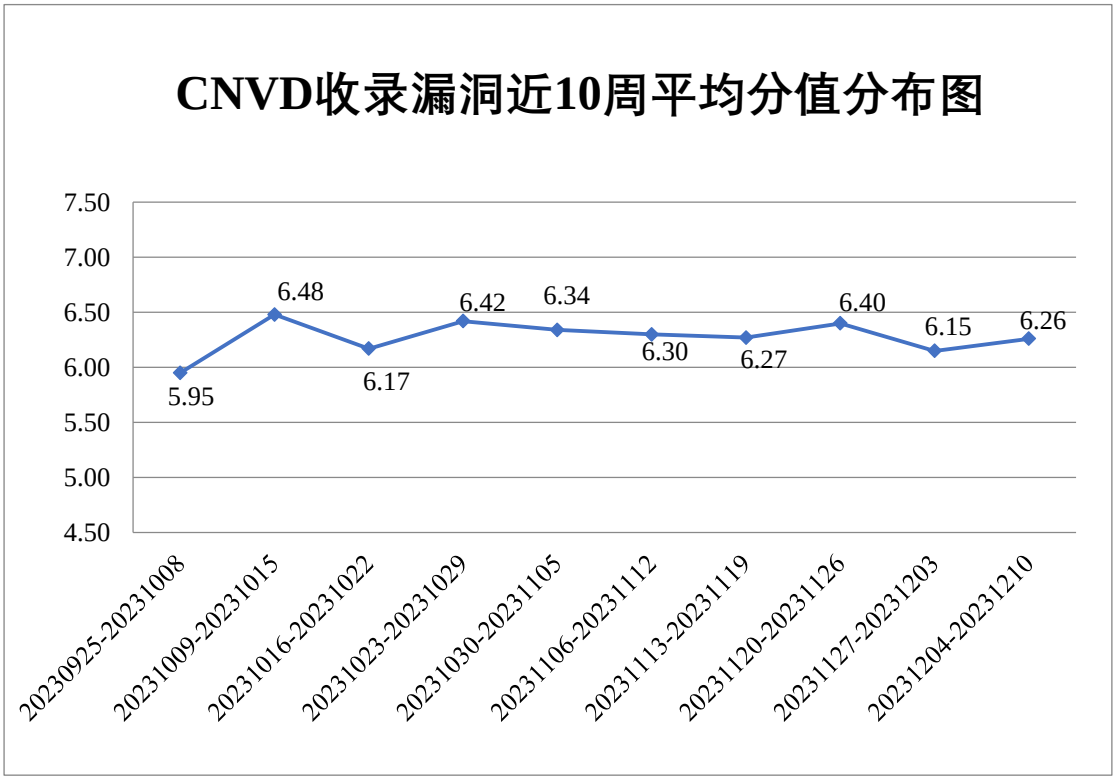

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电信企业通报漏洞事件 13 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 109 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 34 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 41 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：

珠海奔图打印科技有限公司、重庆远通电子技术开发有限公司、众勤通信设备贸易（上海）有限公司、中投国搜（北京）科技股份有限公司、中控技术股份有限公司、智石开工业软件有限公司、郑州三晖电气股份有限公司、郑州单点科技软件有限公司、浙江兰德纵横网络技术股份有限公司、浙江和达科技股份有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、信呼、武汉今客软件有限公司、通州区华丽软件工作室、铁铁智慧物流（天津）有限公司、天津百望金赋科技有限公司、太原易思软件技术有限公司、台达电子企业管理（上海）有限公司、宿迁鑫潮信息技术有限公司、苏州伟创电气科技股份有限公司、苏州科达科技股份有限公司、四川中环盟科技有限公司、陞泰科技股份有限公司、深圳市思迅软件股份有限公司、深圳市三联众瑞科技有限公司、深圳市美科星通信技术有限公司、深圳市蓝凌软件股份有限公司、深圳市科脉技术股份有限公司、深圳市吉祥腾达科技有限公司、深圳市顶讯网络科技有限公司、深圳市道通智能航空技术股份有限公司、上海易正信息技术有限公司、上海延华智能科技（集团）股份有限公司、上海澍品信息科技有限公司、上海市政工程设计研究总院（集团）有限公司、上海荃路软件开发工作室、上海普华科技发展股份有限公司、上海穆云智能科技有限公司、上海罗湖斯自动化技术有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海百胜软件股份有限公司、上海艾泰科技有限公司、陕西小伙伴网络科技有限公司、山西森甲能源科技有限公司、山东思达特测控设备有限公司、厦门正航软件科技有限公司、厦门四信通信科技有限公司、厦门市易联众易惠科技有限公司、厦门南讯股份有限公司、厦门纳龙健康科技股份有限公司、青岛鹏为软件有限公司、普联软件股份有限公司、南京南瑞信通科技有限公司、迈普通信技术股份有限公司、蚂蚁安全响应中心、凌志软件股份有限公司、辽宁畅通数据通信有限公司、联奕科技股份有限公司、联想（北京）有限公司、朗坤智慧科技股份有限公司、廊坊市极致网络科技有限公司、蓝卓数字科技有限公司、兰州中科维智信息咨询有限公司、科大讯飞信息科技股份有限公司、金卡智能集团股份有限公司、金卡银证软件（杭州）有限公司、金蝶软件（中国）有限公司、江苏天捷信息技术有限公司、江苏麦维智能科技有限公司、佳能（中国）有限公司、济南有人物联网技术有限公司、吉翁电子（深圳）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、恒久尚品网络科技（北京）有限公司、杭州雄伟科技开发股份有限公司、杭州合泰软件有限公司、杭州光海科技有限公司、瀚高基础软件股份有限公司、海南赞赞网络科技有限公司、哈尔滨新中新电子股份有限公司、国泰新点软件股份有限公司、广州优胜特软件开发有限公司、广州市德慷电子有限公司、广州市奥威亚电子科技有限公司、广州南方卫星导航仪器有限公司、广州安网通信技术有限公司、广西海豚有海信息科技有限公司、广联达科技股份有限公司、广东伟达智能装备股份有限公司、富士施乐（中国）有限公司、福建科立讯通信有限公司、东莞市通天星软件科技有限公司、东方网力科技股份有限公司、大连华天软件有限公司、成都零起飞网络、成都飞鱼星科技股份有限公司、常州文庭软件有限公司、北京中科聚网信息技术有限公司、北京智慧远景科技产业有限公司、北京致远互联软件股份有限公司、北京亿赛通科技发展有限责任公司、北京炎黄盈动科技发展有限责任公司、北京亚鸿世纪科技发展有限公司、北京星网锐捷网络技术有限公司、北京网动网络科技股份有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京拓尔思信息技术股份有限公司、北京泉江科技有限责任公司、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京春笛网络信息技术服务有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、奥琦玮信息科技（北京）有限公司、安科瑞电气股份有限公司、爱普生（中国）有限公司、SOYAL 茂旭資迅股份有限公司和 PESCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天津市国瑞数码安全系统股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、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。联想集团、北京山石网科信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、贵州多彩网安科技有限公司、中孚安全技术有限公司、河南东方云盾信息技术有限公司、江苏金盾检测技术股份有限公司、内蒙古洞明科技有限公司、江苏百达智慧网络科技有限公司（含光实验室）、快页信息技术有限公司、杭州默安科技有限公司、山石网科通信技术股份有限公司、博智安全科技股份有限公司、北京卓识网安技术股份有限公司、安徽天行网安信息安全技术有限公司、杭州美创科技有限公司、安徽锋刃信息科技有限公司、江苏易安联网络技术有限公司、北京中关村实验室、苏州棱镜七彩信息科技有限公司、北京微步在线科技有限公司、北京天防安全科技有限公司、贵州华黔信安信息技术有限公司、成都安美勤信息技术股份有限公司、江苏省信息安全测评中心、北京君云天下科技有限公司、任子行网络技术股份有限公司、西安交大捷普网络科技有限公司、河南悦海数安科技有限公司、赛尔网络有限公司、广州中科诺泰技术有限公司、宁夏凯信特信息科技有限公司、浙江安腾信息技术有限公司、江苏晟晖信息科技有限公司、上海纽盾科技股

份有限公司、信联科技（南京）有限公司、贵州电网有限责任公司信息中心、中电福富信息科技有限公司、杭州弘沿科技有限公司、西藏熙安信息技术有限责任公司、北京安帝科技有限公司、河南灵创电子科技有限公司、云南联创网安科技有限公司、杭州智顺科技有限公司及其他个人白帽子向 CNVD 提交了 22289 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）、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 20213 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）	11686	11686
奇安信网神（补天平台）	7538	7538
天津市国瑞数码安全系统股份有限公司	2556	0
深信服科技股份有限公司	1434	0
北京天融信网络安全技术有限公司	647	8
新华三技术有限公司	618	0
三六零数字安全科技集团有限公司	530	530
北京启明星辰信息安全技术有限公司	482	28
上海交大	459	459
安天科技集团股份有限公司	362	4
北京神州绿盟科技有限公司	233	0
北京数字观星科技有限公司	199	0
阿里云计算有限公司	174	17
北京知道创宇信息技术有限公司	161	0
杭州安恒信息技术股份有限公司	69	69
北京长亭科技有限公	30	0

司		
中电科网络安全科技股份有限公司	30	0
远江盛邦（北京）网络安全科技股份有限公司	28	28
杭州迪普科技股份有限公司	10	0
京东科技信息技术有限公司	6	6
北京安信天行科技有限公司	3	3
南京联成科技发展股份有限公司	3	3
中国电信股份有限公司网络安全产品运营中心	1	1
北京信联数安科技有限公司	1	1
联想集团	127	127
北京山石网科信息技术有限公司	82	82
奇安星城网络安全运营服务（长沙）有限公司	79	79
贵州多彩网安科技有限公司	45	45
中孚安全技术有限公司	39	39
河南东方云盾信息技术有限公司	38	38
江苏金盾检测技术股份有限公司	27	27
内蒙古洞明科技有限公司	22	22

江苏百达智慧网络科技有限公司（含光实验室）	19	19
快页信息技术有限公司	18	18
杭州默安科技有限公司	13	13
山石网科通信技术股份有限公司	10	10
博智安全科技股份有限公司	8	8
北京卓识网安技术股份有限公司	8	8
安徽天行网安信息安全技术有限公司	7	7
杭州美创科技有限公司	6	6
安徽锋刃信息科技有限公司	6	6
江苏易安联网络技术有限公司	6	6
北京中关村实验室	5	5
苏州棱镜七彩信息科技有限公司	4	4
北京微步在线科技有限公司	3	3
北京天防安全科技有限公司	3	3
贵州华黔信安信息技术有限公司	3	3
成都安美勤信息技术股份有限公司	3	3
江苏省信息安全测评中心	2	2
北京君云天下科技有	2	2

限公司		
任子行网络技术股份有限公司	2	2
西安交大捷普网络科技有限公司	1	1
河南悦海数安科技有限公司	1	1
赛尔网络有限公司	1	1
广州中科诺泰技术有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
浙江安腾信息技术有限公司	1	1
江苏晟晖信息科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
信联科技（南京）有限公司	1	1
贵州电网有限责任公司信息中心	1	1
中电福富信息科技有限公司	1	1
杭州弘沿科技有限公司	1	1
西藏熙安信息技术有限责任公司	1	1
北京安帝科技有限公司	1	1
河南灵创电子科技有限公司	1	1
云南联创网安科技有限公司	1	1
杭州智顺科技有限公	1	1

司		
CNCERT 广西分中心	5	5
CNCERT 贵州分中心	1	1
个人	1298	1298
报送总计	29168	22289

本周漏洞按类型和厂商统计

本周，CNVD 收录了 531 个漏洞。WEB 应用 270 个，应用程序 124 个，网络设备（交换机、路由器等网络端设备）76 个，智能设备（物联网终端设备）30 个，操作系统 15 个，安全产品 9 个，数据库 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	270
应用程序	124
网络设备（交换机、路由器等网络端设备）	76
智能设备（物联网终端设备）	30
操作系统	15
安全产品	9
数据库	7

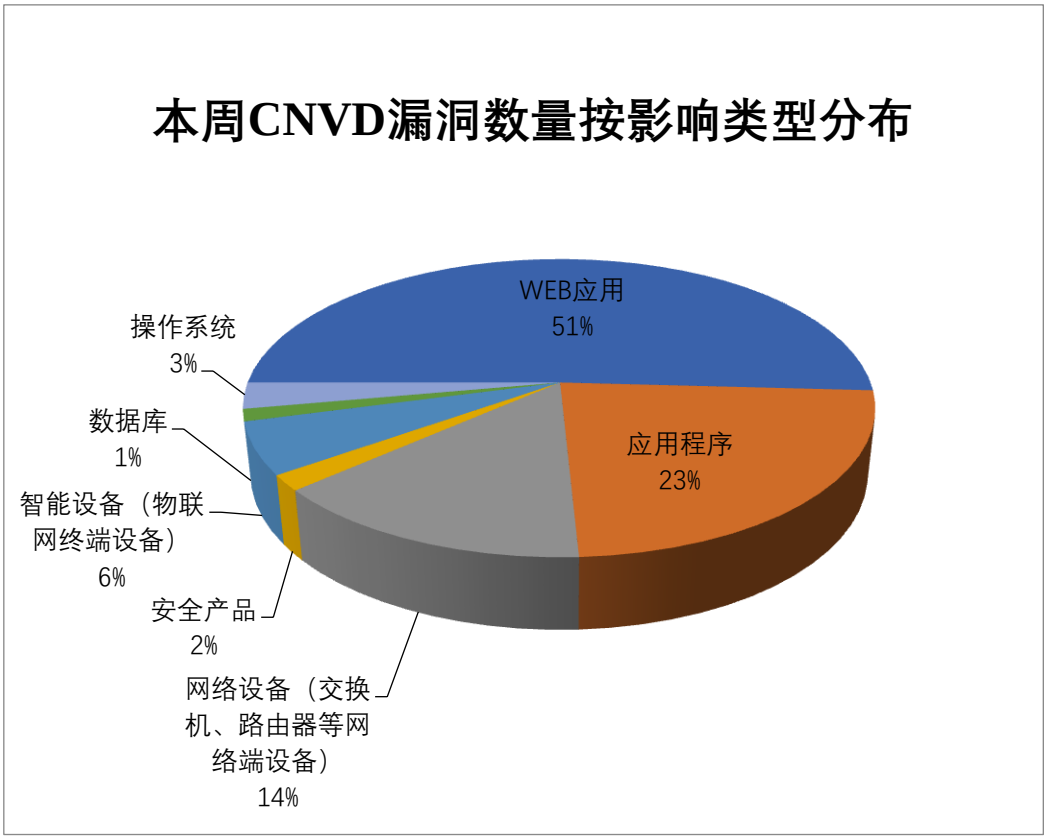

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、WordPress、北京星网锐捷网络技术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	IBM	19	4%
2	WordPress	18	3%
3	北京星网锐捷网络技术有限公司	20	4%
4	Samsung	12	2%
5	用友网络科技股份有限公司	12	2%
6	Adobe	12	2%
7	Google	11	2%
8	北京百卓网络技术有限公司	11	2%
9	Foxit	8	2%
10	其他	408	77%

本周行业漏洞收录情况

本周，CNVD 收录了 36 个电信行业漏洞，55 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2023-96077、CNVD-2023-96079）”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/

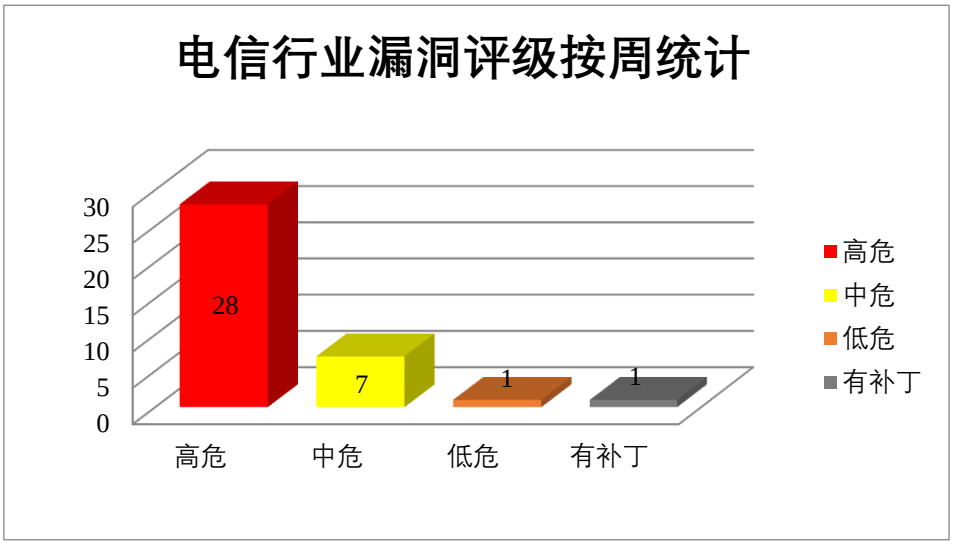

图 3 电信行业漏洞统计

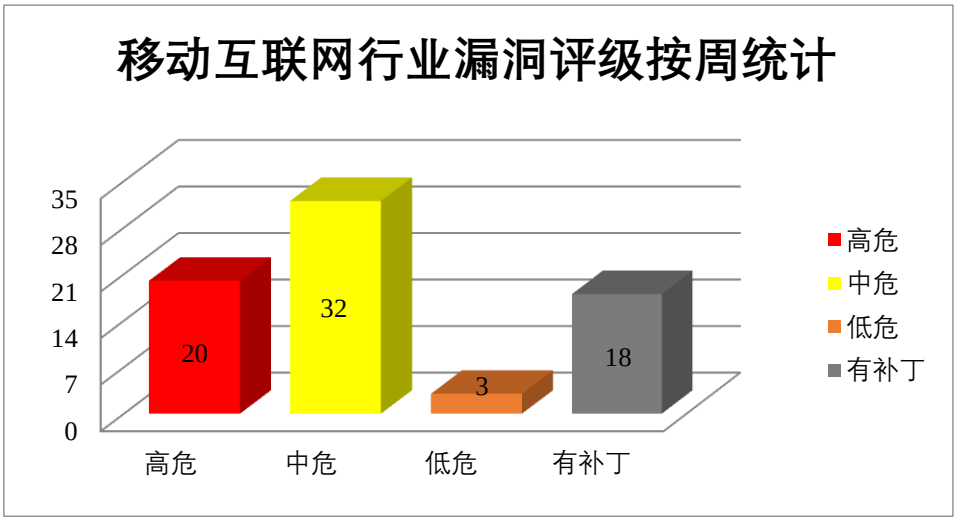

图 4 移动互联网行业漏洞统计

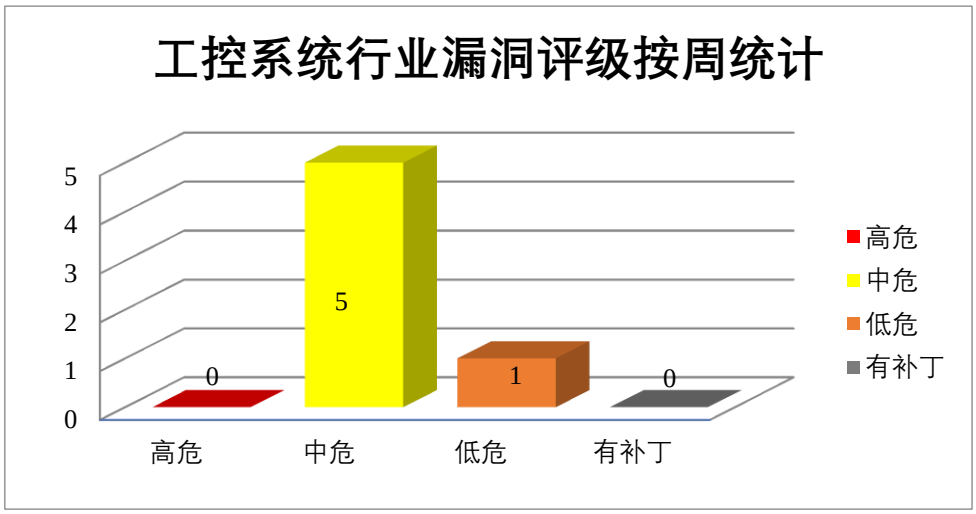

图 5 工控系统行业漏洞统计

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，攻击者可利用漏洞获取敏感信息，在系统上获得提升的权限。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-96075、CNVD-2023-96077、CNVD-2023-96079、CNVD-2023-96080、CNVD-2023-96081、CNVD-2023-96082、CNVD-2023-96084）、Google Android 信息泄露漏洞（CNVD-2023-96083）。其中，除“Google Android 信息泄露漏洞（CNVD-2023-96083）”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-2023-96075
https://www.cnvd.org.cn/flaw/show/CNVD-2023-96077
https://www.cnvd.org.cn/flaw/show/CNVD-2023-96079
https://www.cnvd.org.cn/flaw/show/CNVD-2023-96080
https://www.cnvd.org.cn/flaw/show/CNVD-2023-96081
https://www.cnvd.org.cn/flaw/show/CNVD-2023-96082
https://www.cnvd.org.cn/flaw/show/CNVD-2023-96083
https://www.cnvd.org.cn/flaw/show/CNVD-2023-96084

2、 Adobe 产品安全漏洞

Adobe Premiere Pro 是美国奥多比（Adobe）公司的一套非线性编辑的视频剪辑软件。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。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，在当前用户的上下文中执行代码，或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Adobe Premiere Pro 越界读取漏洞（CNVD-2023-95449、CNVD-2023-95448）、Adobe Premiere Pro 缓冲区溢出漏洞（CNVD-2023-95451）、Adobe Premiere Pro 越界写入漏洞（CNVD-2023-95450）、Adobe Photoshop 越界读取漏洞（CNVD-2023-95524、CNVD-2023-95528、CNVD-2023-95526、CNVD-2023-95525）。其中，“Adobe Premiere Pro 越界读取漏洞（CNVD-2023-95449、CNVD-2023-95448）、Adobe Premiere Pro 缓冲区溢出漏洞（CNVD-2023-95451）、Adobe Premiere Pro 越界写入漏洞（CNVD-2023-95450）”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-2023-95449

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95448

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95451

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95450

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95524

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95528

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95526

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95525

3、IBM 产品安全漏洞

IBM CICS TX 是美国国际商业机器（IBM）公司的一个综合的、单一的事务运行时包。IBM Cloud Pak for Security 是美国国际商业机器（IBM）公司的一款应用软件。一个开放的安全平台，可连接到您现有的数据源以产生更深刻的见解，并使您能够更快地采取自动化行动。IBM Sterling Partner Engagement Manager（PEM）是一种供应链合作伙伴管理解决方案，可以为企业和其供应链合作伙伴带来提高效率和准确性、增强可见性和透明度等。IBM AIX（Advanced Interactive eXecutive）是 IBM 公司开发的基于 UNIX 的操作系统。IBM Security Verify Governance 是美国国际商业机器（IBM）公司的一个智能身份访问平台。为组织提供了一个平台来分析、定义和控制用户访问和访问风险。IBM InfoSphere Information Server 是美国国际商业机器（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。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，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM CICS TX Advanced 弱算法漏洞、IBM Cloud Pak for Security and IBM QRadar Suite Software 信息泄露漏洞、IBM Sterling Partner Engagement Manager 跨站脚本漏洞（CNVD-2023-95294）、IBM AIX 拒绝服务漏洞（CNVD-2023-95293）、IBM CICS TX 跨站请求伪造漏洞（CNVD-2023-95292）、IBM CICS TX 跨站脚本漏洞（CNVD-2023-95291）、IBM Security Verify Governance 硬编码漏洞、IBM InfoSphere Information Server 输入验证错误漏洞。其中，“IBM CICS TX Advanced 弱算法漏洞、IBM InfoSphere Information Server 输入验证错误漏洞”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-2023-95290

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95288

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95294

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95293

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95292

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95291

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95295

https://www.cnvd.org.cn/flaw/show/CNVD-2023-95713

4、Foxit 产品安全漏洞

Foxit Reader 是中国福昕（Foxit）公司的一款 PDF 文档阅读器。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执行任意代码等。

CNVD 收录的相关漏洞包括：Foxit Reader 任意文件创建漏洞（CNVD-2023-96087、CNVD-2023-96090）、Foxit Reader 类型混淆漏洞（CNVD-2023-96088）、Foxit Reader 代码执行漏洞（CNVD-2023-96089、CNVD-2023-96093）、Foxit Reader 内存错误引用漏洞（CNVD-2023-96091、CNVD-2023-96092、CNVD-2023-96094）。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-2023-96087

https://www.cnvd.org.cn/flaw/show/CNVD-2023-96088

https://www.cnvd.org.cn/flaw/show/CNVD-2023-96089

https://www.cnvd.org.cn/flaw/show/CNVD-2023-96090

https://www.cnvd.org.cn/flaw/show/CNVD-2023-96091

https://www.cnvd.org.cn/flaw/show/CNVD-2023-96092

https://www.cnvd.org.cn/flaw/show/CNVD-2023-96093

https://www.cnvd.org.cn/flaw/show/CNVD-2023-96094

5、Open5GS 拒绝服务漏洞（CNVD-2023-96086）

Open5GS 是一个 5G Core 和 Epc 的 C 语言开源实现，即 Lte/Nr 网络的核心网络。本周，Open5GS 被披露存在拒绝服务漏洞。该漏洞是由于 ogs_sbi_message_free 函数中的无效指针释放缺陷，攻击者可利用该漏洞导致服务中断。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-2023-96086

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-2023-95527	Adobe Photoshop 越界写入漏洞（CNVD-2023-95527）	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/photoshop/apsb23-56.html
CNVD-2023-95339	WordPress Bello-Directory&Listing theme 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/731

			4f9fa-c047-4e0c-b145-940240a50c02
CNVD-2023-96076	Google Android Framework 权限提升漏洞（CNVD-2023-96076）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/docs/security/bulletin/android-14
CNVD-2023-95341	openSUSE Factory 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.opensuse.org/
CNVD-2023-96092	Foxit Reader 内存错误引用漏洞（CNVD-2023-96092）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/downloads/
CNVD-2023-95346	WordPress PublishPress Capabilities 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://wpscan.com/vulnerability/2f0f1a32-0c7a-48e6-8617-e0b2dcf62727
CNVD-2023-95448	Adobe Premiere Pro 越界读取漏洞（CNVD-2023-95448）	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/premiere_pro/apsb23-65.html
CNVD-2023-96078	Google Android Framework 权限提升漏洞（CNVD-2023-96078）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/docs/security/bulletin/android-14
CNVD-2023-96089	Foxit Reader 代码执行漏洞（CNVD-2023-96089）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/downloads/
CNVD-2023-96074	Google Android 权限提升漏洞（CNVD-2023-96074）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/docs/security/bulletin/android-14

小结：本周，Google 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，在系统上获得提升的权限。此外，Adobe、IBM、Foxit 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，在当前用户的上下文中执行代码，导致拒绝服务等。另外，Open5GS 被披露存在拒绝服务漏洞。攻击者可利用漏洞导致服务中断。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、PortlandLabs Concrete CMS 自定义标签字段跨站脚本漏洞

验证描述

PortlandLabs Concrete CMS 是美国 PortlandLabs 公司的一个面向团队的开源内容管理系统。

PortlandLabs Concrete CMS 自定义标签字段存在跨站脚本漏洞，该漏洞源于数据对象的表单的“自定义标签”字段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通过注入设计的有效载荷执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/sromanhu/CVE-2023-44761_ConcreteCMS-Stored-XSS--Forms

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-96085

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. 现已修复！WordPress 曝出安全漏洞

Bleeping Computer 网站消息，WordPress 近期发布了 6.4.2 更新版本，修复了一个远程代码执行 (RCE) 漏洞。据悉，该漏洞能够与另外一个安全漏洞形成“联动”，允许威胁攻击者在目标网站上运行任意 PHP 代码。

参考链接：https://www.freebuf.com/news/386057.html

2. Sierra 安全漏洞影响基础设施

研究人员发现了 21 个安全漏洞，这些漏洞会影响 Sierra OT/IoT 路由器，威胁攻击者能够利用漏洞，通过远程代码执行、未授权访问、跨站脚本、身份验证绕过和拒绝服务攻击袭击基础设施。

参考链接：https://www.bleepingcomputer.com/news/security/sierra-21-vulnerabilities-impact-critical-infrastructure-routers/

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