国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 06 月 19 日-2023 年 06 月 25 日 **2023 年第 25 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 308 个，其中高危漏洞 207 个、中危漏洞 93 个、低危漏洞 8 个。漏洞平均分值为 7.05。本周收录的漏洞中，涉及 0day 漏洞 241 个（占 78%），其中互联网上出现“Tenda AC 10 堆栈缓冲区溢出漏洞、iKuai8 命令注入漏洞”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 9819 个，与上周（14881 个）环比减少 34%。

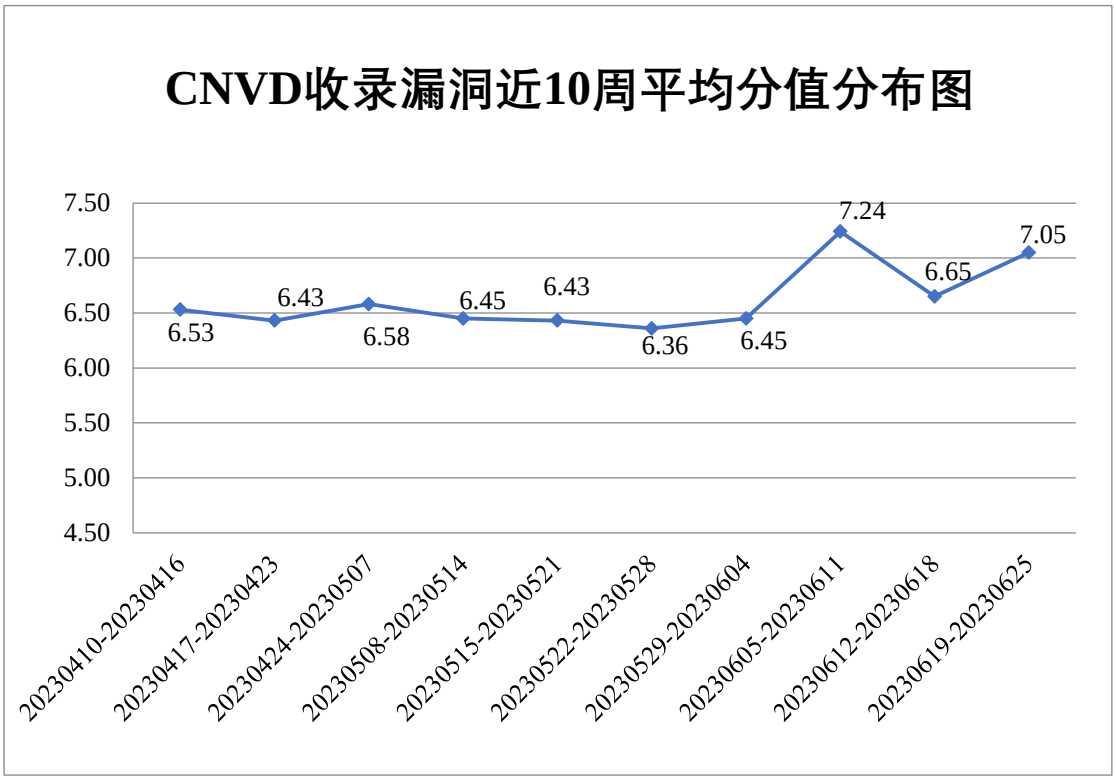

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 起，向基础电信企业通报漏洞事 21 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 1068 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 282 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 42 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、中国华能集团有限公司、郑州微厦计算机科技有限公司、正奇晟业（北京）科技有限公司、浙江创邻科技有限公司、长沙米拓信息技术有限公司、长沙德尚网络科技有限公司、用友网络科技股份有限公司、项城市梦远医疗科技有限公司、西安华谊云信息科技有限公司、武汉天地伟业科技有限公司、武汉简码科技有限公司、卫宁健康科技集团股份有限公司、潍坊雷鸣云网络科技有限公司、天津天堰科技股份有限公司、天津谷川科技有限公司、天津顶巧餐饮服务咨询有限公司、梯子数字文化扬州有限公司、台达电子企业管理（上海）有限公司、四川众望升腾科技有限公司、四川蜀天梦图数据科技有限公司、石家庄市征红网络科技有限公司、深圳市吉祥腾达科技有限公司、深圳市海融易通电子有限公司、深圳市从晶科技有限公司、深圳市必联电子有限公司、深圳市安佳威视信息技术有限公司、深圳科士达科技股份有限公司、深信服科技股份有限公司、上海商派网络科技有限公司、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、上海百胜软件股份有限公司、熵基科技股份有限公司、商派软件有限公司、山东威尔数据股份有限公司、山东农友软件有限公司、山东金钟科技集团股份有限公司、山东国通智云实业集团有限公司、厦门同迈科技有限公司、厦门四信通信科技有限公司、任子行网络技术股份有限公司、亲祥源（山东）健康产业集团有限公司、宁波迪泰电子科技有限公司、泸州能源投资有限公司、龙采科技集团有限责任公司、乐鑫信息科技（上海）股份有限公司、浪潮通用软件有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、湖南元想科技有限公司、湖南强智科技发展有限公司、湖南快乐车行露营地投资发展有限公司、湖北点点点科技有限公司、湖北楚天智能交通股份有限公司、河北赢图网络科技有限公司、合肥天寻信息科技有限公司、杭州佐巨网络科技有限公司、杭州先锋电子技术股份有限公司、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、广州图创计算机软件开发有限公司、广东保伦电子股份有限公司、帆软软件有限公司、帝国软件、成都索贝数码科技股份有限公司、北京众智联创科技有限公司、北京中科网威信息技术有限公司、北京致远互联软件股份有限公司、北京用友政务软件股份有限公司、北京星网锐捷网络技术有限公司、北京网康科技有限公司、北京通达信科科技有限公司、北京睿智融科控股股份有限公司、北京人人微聘科技有限公司、北京南琼电子有限责任公司、北京龙软科技股份有限公司、北京宏景世纪软件股份有限公司、北京超图软件股份有限公司、北京北大方正电子有限

公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、安吉加加信息技术有限公司、安徽青柿信息科技有限公司、Trend Micro Incorporated.和 jeewms。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、安天科技集团股份有限公司、深信服科技股份有限公司、阿里云计算有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。杭州海康威视数字技术股份有限公司、北京升鑫网络科技有限公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、重庆电信系统集成公司、联想集团、河南信安世纪科技有限公司、内蒙古中叶信息技术有限责任公司、上海齐同信息科技有限公司、安徽锋刃信息科技有限公司、杭州美创科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、杭州默安科技有限公司、北京时代新威信息技术有限公司、北京山石网科信息技术有限公司、浙江海瑞网络科技有限公司、山东正中信息技术股份有限公司、赛尔网络有限公司、博智安全科技股份有限公司、河北锎远网络科技有限公司、西藏熙安信息技术有限责任公司、广州安亿信软件科技有限公司、河南省鼎信信息安全等级测评有限公司、山东谷联网络技术有限公司、河南灵创电子科技有限公司、北京众安天下科技有限公司、长春嘉诚信息技术股份有限公司、贵州多彩网安科技有限公司、中科国宏科技有限公司、北京微步在线科技有限公司、北京君云天下科技有限公司、重庆易阅科技有限公司、江苏晟晖信息科技有限公司、亚信科技（成都）有限公司、奇安信-工控安全实验室及其他个人白帽子向 CNVD 提交了 9819 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 7959 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）	3377	3377
斗象科技（漏洞盒子）	3299	3299
三六零数字安全科技集团有限公司	849	849
上海交大	434	434
新华三技术有限公司	353	0
安天科技集团股份有限公司	320	0
深信服科技股份有限	279	2

公司		
阿里云计算有限公司	144	0
北京数字观星科技有限公司	111	0
北京启明星辰信息安全技术有限公司	99	2
远江盛邦（北京）网络安全科技股份有限公司	43	43
中国电信集团系统集成有限责任公司	18	0
京东科技信息技术有限公司	10	0
杭州迪普科技股份有限公司	10	0
北京天融信网络安全技术有限公司	5	5
卫士通信息产业股份有限公司	2	2
浙江大华技术股份有限公司	2	2
北京长亭科技有限公司	1	1
北京信联数安科技有限公司	1	1
北京智游网安科技有限公司	1	1
西安四叶草信息技术有限公司	1	1
北京知道创宇信息技术股份有限公司	1	0
杭州海康威视数字技术股份有限公司	93	93
北京升鑫网络科技有限公司	92	92

河南东方云盾信息技术有限公司	69	69
快页信息技术有限公司	69	69
重庆电信系统集成公司	43	43
联想集团	26	26
河南信安世纪科技有限公司	24	24
内蒙古中叶信息技术有限责任公司	20	20
上海齐同信息科技有限公司	20	20
安徽锋刃信息科技有限公司	19	19
杭州美创科技有限公司	17	17
北京云科安信科技有限公司（Seraph 安全实验室）	7	7
杭州默安科技有限公司	7	7
北京时代新威信息技术有限公司	5	5
北京山石网科信息技术有限公司	5	5
浙江海瑞网络科技有限公司	4	4
山东正中信息技术股份有限公司	4	4
赛尔网络有限公司	2	2
博智安全科技股份有限公司	2	2
河北锎远网络科技有限公司	2	2

西藏熙安信息技术有限责任公司	1	1
广州安亿信软件科技有限公司	1	1
河南省鼎信信息安全等级测评有限公司	1	1
山东谷联网络技术有限公司	1	1
河南灵创电子科技有限公司	1	1
北京众安天下科技有限公司	1	1
长春嘉诚信息技术股份有限公司	1	1
贵州多彩网安科技有限公司	1	1
中科国宏科技有限公司	1	1
北京微步在线科技有限公司	1	1
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
江苏晟晖信息科技有限公司	1	1
亚信科技（成都）有限公司	1	1
奇安信-工控安全实验室	1	1
CNCERT 河北分中心	11	11
CNCERT 内蒙古分中心	3	3
个人	1241	1241
报送总计	11160	9819

本周漏洞按类型和厂商统计

本周，CNVD 收录了 308 个漏洞。WEB 应用 170 个，应用程序 76 个，网络设备（交换机、路由器等网络端设备）48 个，操作系统 10 个，智能设备（物联网终端设备 4 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	170
应用程序	76
网络设备（交换机、路由器等网络端设备）	48
操作系统	10
智能设备（物联网终端设备）	4

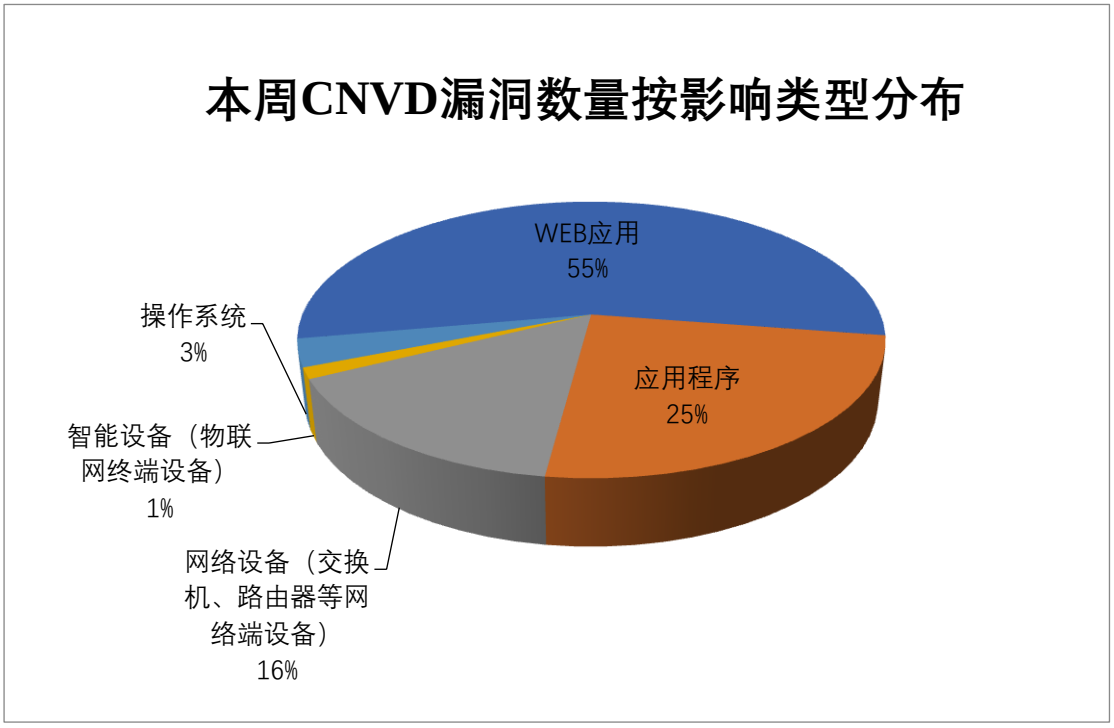

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Google、Foxit 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	Adobe	21	7%
2	Google	17	6%
3	Foxit	10	3%
4	Tenda	10	3%

5	Rockwell Automation	9	3%
6	H3C	6	2%
7	睿因科技（深圳）有限公司	5	2%
8	TOTOLINK	4	1%
9	Cab Management System	4	1%
10	其他	222	72%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，31 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Rockwell Automation Arena Simulation Software 缓冲区溢出漏洞、Google Android 权限提升漏洞（CNVD-2023-50310）”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/

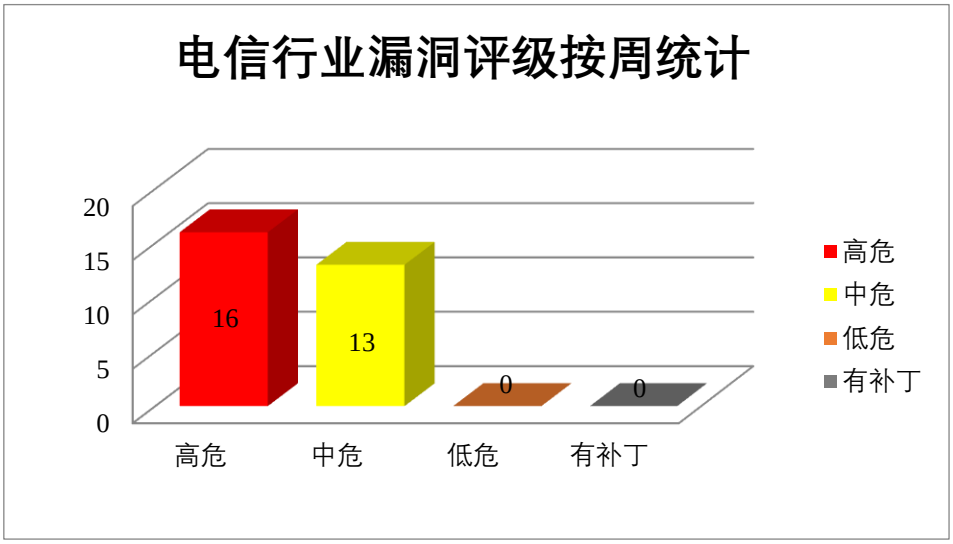

图 3 电信行业漏洞统计

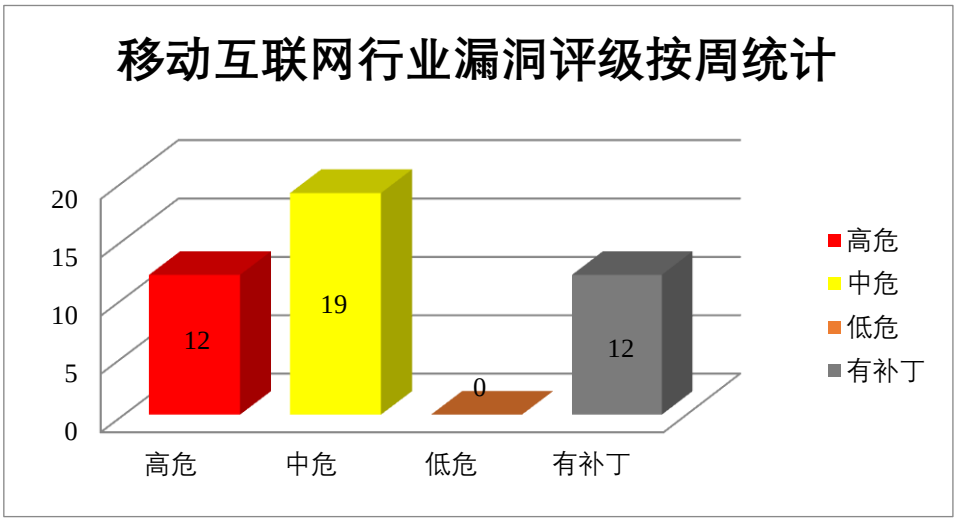

图 4 移动互联网行业漏洞统计

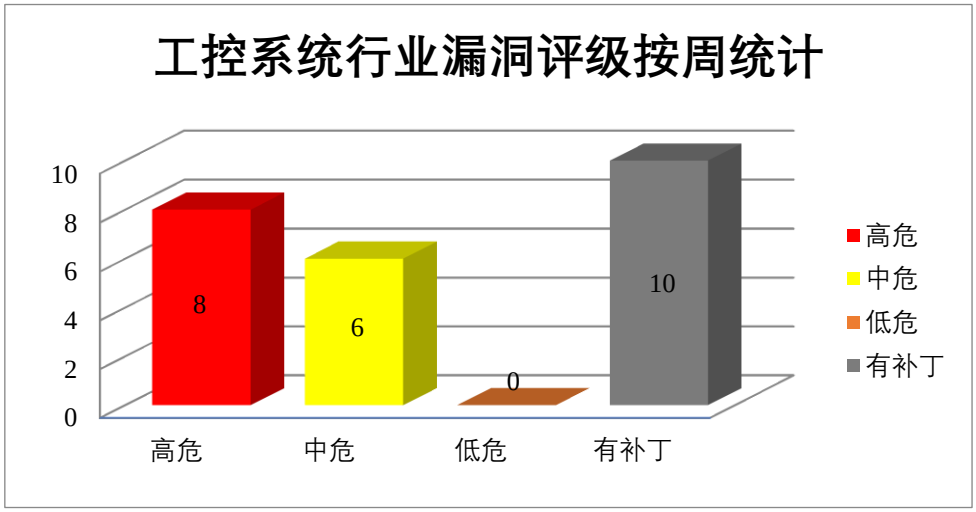

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的数字商务解决方案。Adobe Premiere Rush 是美国奥多比（Adobe）公司的一套跨平台的视频编辑软件。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。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。Adobe Creative Cloud Desktop Application 是美国奥多比（Adobe）公司的一套用于在 Creative 云会员管理中心管理应用程序和服务的应用程序。该程序支持同步和共享文件、管理字体以及访问商业摄影和设计的资产库。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安全功能，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Commerce 任意代码执行漏洞、Adobe Commerce 安全绕过漏洞（CNVD-2023-50130）、Adobe Premiere Rush 内存错误引用漏洞、Adobe Photoshop 内存错误引用漏洞、Adobe Illustrator 越界写入漏洞（CNVD-2023-50820、CNVD-2023-50822）、Adobe Illustrator 代码执行漏洞（CNVD-2023-50821）、Adobe Creative Cloud Desktop Application 代码执行漏洞。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-2023-50124
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50130
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50814
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50817
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50820
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50821
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50822
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50823

2、Foxit 产品安全漏洞

Foxit PDF Reader 是中国福昕（Foxit）公司的一款 PDF 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当前进程的上下文中执行代码，造成拒绝服务（DoS）。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 拒绝服务漏洞、Foxit PDF Reader 资源管理错误漏洞（CNVD-2023-49833、CNVD-2023-49832、CNVD-2023-49836、CNVD-2023-49835、CNVD-2023-49834）、Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2023-49839、CNVD-2023-49838）。其中，除“Foxit PDF Reader 拒绝服务漏洞、Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2023-49838）”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-2023-49829
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49833
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49832
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49836
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49835
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49834
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49839
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49838

3、Rockwell Automation 产品安全漏洞

Rockwell Automation Kinetix 5500 是美国罗克韦尔（Rockwell Automation）公司的第一款采用外部公共交流/直流总线连接系统设计的 Kinetix 驱动器。它降低了硬件要求，并允许无缝扩展，对单轴或多轴系统使用单一平台。Rockwell Automation Arena Simulation Software 是美国罗克韦尔（Rockwell Automation）公司的一套提供 3D 动画和图形功能的仿真软件。Rockwell Automation FactoryTalk Vantagepoint 是美国罗克韦尔（Rockwell Automation）公司的在统一生产模型（UPM）中组织、关联和规范化制造和生产流程以及业务系统的不同数据的平台。Rockwell Automation ThinManager ThinServer 是美国罗克韦尔（Rockwell Automation）公司的一款瘦客户端管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过开放端口未经授权访问设备，远程执行任意代码，导致程序崩溃等。

CNVD 收录的相关漏洞包括：Rockwell Automation Kinetix 5500 访问控制错误漏洞、Rockwell Automation Arena Simulation Software 缓冲区溢出漏洞（CNVD-2023-49823、CNVD-2023-49822、CNVD-2023-49821）、Rockwell Automation FactoryTalk Vantagepoint 跨站请求伪造漏洞、Rockwell Automation ThinManager ThinServer 路径遍历漏洞（CNVD-2023-49827、CNVD-2023-49826）、Rockwell Automation ThinManager ThinServer 缓冲区溢出漏洞。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-2023-49819
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49823
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49822
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49821
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49820
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49827
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49826
https://www.cnvd.org.cn/flaw/show/CNVD-2023-49825

4、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，提升权限，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-50309、CNVD-2023-50310、CNVD-2023-50311、CNVD-2023-50829、CNVD-2023-50830）、Google Android 拒绝服务漏洞（CNVD-2023-50826）、Google Android 信息泄露漏洞（CNVD-2023-50827、CNVD-2023-50828）。其中，除“Google Android 信息泄露漏洞（CNVD-2023-50827、CNVD-2023-50828）”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-2023-50309
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50310
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50311
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50826
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50827
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50828
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50829
https://www.cnvd.org.cn/flaw/show/CNVD-2023-50830

5、D-Link DIR-600 命令注入漏洞

D-Link DIR-600 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-600 被披露存在命令注入漏洞。该漏洞源于 lxmldbc_system()函数中的 ST 参数未能正确过滤构造命令特殊字符、命令等。攻击者可利用此漏洞导致任意命令执行。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-2023-50813

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-2023-49821	Rockwell Automation Arena Simulation Software 缓冲区溢出漏洞（CNVD-2023-49821）	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/1139391
CNVD-2023-49836	Foxit PDF Reader 资源管理错误漏洞（CNVD-2023-49836）	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.foxit.com/support/security-bulletins.html
CNVD-2023-49841	PrestaShop 路径遍历漏洞（CNVD-2023-49841）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/PrestaShop/PrestaShop/blob/6c05518b807d014ee8edb811041e3de232520c28/classes/Tools.php#L1247
CNVD-2023-50824	Adobe Substance 3D Stager 堆缓冲区溢出漏洞（CNVD-2023-50824）	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/prod

			ucts/substance3d_stager/apsb23-22.html
CNVD-2023-50311	Google Android 权限提升漏洞（CNVD-2023-50311）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2023-04-01
CNVD-2023-50817	Adobe Photoshop 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://helpx.adobe.com/security/products/photoshop/apsb23-23.html
CNVD-2023-50830	Google Android 权限提升漏洞（CNVD-2023-50830）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2023-06-01
CNVD-2023-49826	Rockwell Automation ThinManager ThinServer 路径遍历漏洞（CNVD-2023-49826）	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/1138640
CNVD-2023-49834	Foxit PDF Reader 资源管理错误漏洞（CNVD-2023-49834）	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.foxit.com/support/security-bulletins.html
CNVD-2023-50822	Adobe Illustrator 越界写入漏洞（CNVD-2023-50822）	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/apsb23-19.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全功能，在系统上执行任意代码。此外，Foxit、Rockwell Automation、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过开放端口未经授权访问设备，获取敏感信息，提升权限，在当前进程的上下文中执行代码，造成拒绝服务等。另外，D-Link DIR-600 被披露存在命令注入漏洞，攻击者可利用此漏洞导致任意命令执行。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 AC10 堆栈缓冲区溢出漏洞

验证描述

Tenda AC10 是一款无线路由器。

Tenda AC10 存在堆栈缓冲区溢出漏洞，该漏洞是由于 addWifiMacFilter 函数未能正

确边界检查引起的。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/z1r00/IOT_Vul/blob/main/Tenda/AC10/addWifiMacFilter/readme.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-50810

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. Zyxel 修复了 NAS 设备中的安全漏洞

近日，Zyxel 针对 CVE-2023-27992（CVSS 评分：9.8）发布了安全更新，这个安全漏洞影响到了其网络附加存储（NAS）设备。

参考链接：https://www.freebuf.com/news/370009.html

2. 华硕曝路由器的安全漏洞

近日，华硕针对多种路由器型号的漏洞，发布了安全固件更新，并敦促客户立即更新设备或限制 WAN 访问，以保证其设备安全。

参考链接：https://www.freebuf.com/news/369912.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