国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 04 月 10 日-2023 年 04 月 16 日 **2023 年第 15 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 446 个，其中高危漏洞 243 个、中危漏洞 173 个、低危漏洞 30 个。漏洞平均分值为 6.53。本周收录的漏洞中，涉及 0day 漏洞 391 个（占 88%），其中互联网上出现“Tenda RX 9 Pro setIPv6Status 缓冲区溢出漏洞、Bento4 拒绝服务漏洞（CNVD-2023-27653）”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 9435 个，与上周（15177 个）环比减少 38%。

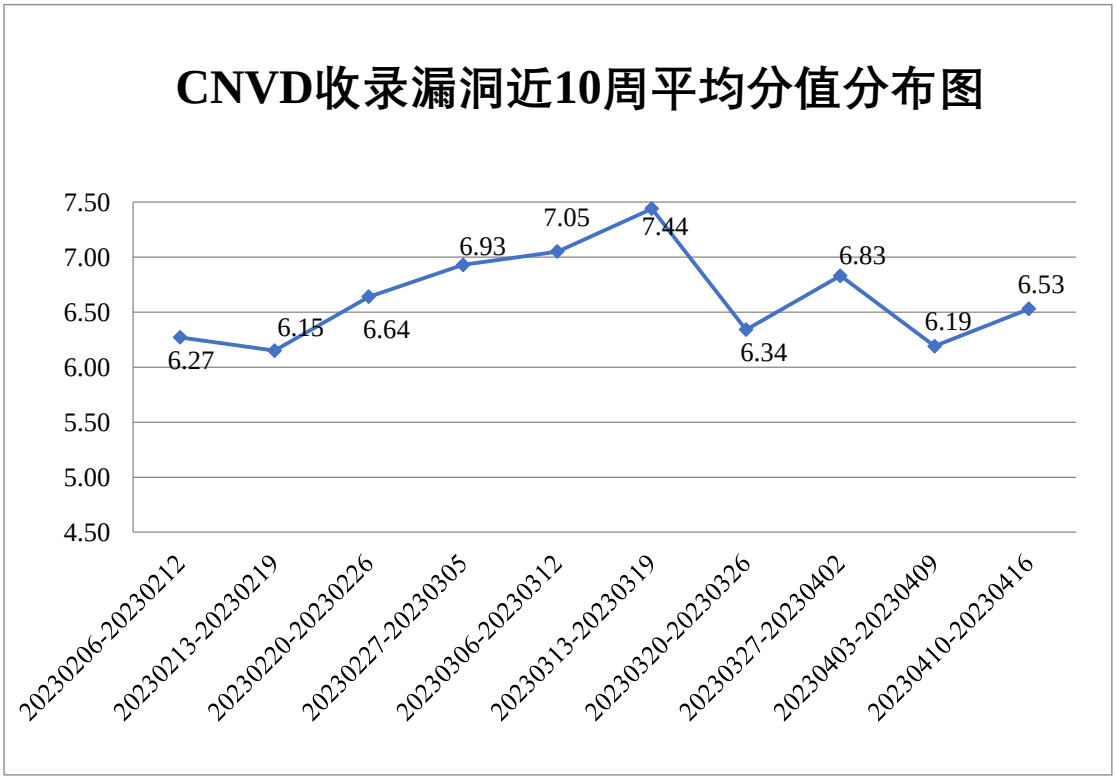

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 41 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 595 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 169 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 68 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：

珠海派诺科技股份有限公司、珠海金山办公软件有限公司、重庆森鑫炬科技有限公司、中科数字通（北京）科技有限公司、中科美络科技股份有限公司、郑州天迈科技股份有限公司、浙江花田网络有限公司、云知声智能科技股份有限公司、云宏信息科技股份有限公司、阳光智园科技有限公司、熊猫智慧水务有限公司、西安卓立科技实业有限公司、武汉慧谷通信技术有限公司、卫宁健康科技集团股份有限公司、宿迁鑫潮信息技术有限公司、苏州汇川技术有限公司、数篷科技（深圳）有限公司、石家庄威大特测控工程有限公司、深圳友联科技有限公司、深圳拓安信物联股份有限公司、深圳搜豹网络有限公司、深圳市锐明技术股份有限公司、深圳市酷开网络科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳市道尔智控科技股份有限公司、深圳市丛文科技有限公司、深圳市必联电子有限公司、深圳市百为通达科技有限公司、上海卓卓网络科技有限公司、上海威派格智慧水务股份有限公司、上海梦创双杨数据科技股份有限公司、上海联泰基金销售有限公司、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、上海楚果信息技术有限公司、上海博达数据通信有限公司、商丘芝麻开门网络科技有限公司、山东中维世纪科技股份有限公司、山东金钟科技集团股份有限公司、力软信息技术（苏州）有限公司、江苏卓易信息科技股份有限公司、江苏安科瑞电器制造有限公司、吉翁电子（深圳）有限公司、湖南乔伦科技有限公司、湖北泰跃卫星技术发展股份有限公司、河南云智互联科技有限公司、杭州易软共创网络科技有限公司、杭州新中大科技股份有限公司、杭州西软信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州藏茗山科技有限公司、国泰新点软件股份有限公司、桂林零与壹软件有限公司、广州市领课网络科技有限公司、广州市和丰自动化科技有限公司、广州红帆科技有限公司、广州高新兴机器人有限公司、广州德生智能信息技术有限公司、广联达科技股份有限公司、广东中硕能源科技有限公司、广东凯格科技有限公司、广东飞企互联科技股份有限公司、福州联迅信息科技有限公司、东莞市虹华软件科技有限公司、鼎捷软件股份有限公司、大连久鹏电子系统工程有限公司、畅捷通信息技术股份有限公司、北京中软国际教育科技股份有限公司、北京用友政务软件股份有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京心海导航教育科技股份有限公司、北京通达信科科技有限公司、北京胜能能源科技有限公

司、北京山石网科信息技术有限公司、北京润乾信息系统技术有限公司、北京墨云科技有限公司、北京六方云信息技术有限公司、北京灵州网络技术有限公司、北京蓝卫通科技有限公司、北京旷视科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京瀚维特科技有限公司、北京国炬信息技术有限公司、北京东方通科技股份有限公司、北京碧海威科技有限公司、北京百卓网络技术有限公司、半月谈新媒体科技有限公司、安徽旭帆信息科技有限公司、WAVLINK、POLYCOM 通讯系统（北京）有限公司、PHPCMS 和《中国学术期刊（光盘版）》电子杂志社有限公司。

本周，CNVD 发布了《Microsoft 发布 2023 年 4 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8756

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、新华三技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、厦门服云信息科技有限公司、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。快页信息技术有限公司、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、河南信安世纪科技有限公司、博智安全科技股份有限公司、安徽锋刃信息科技有限公司、河南东方云盾信息技术有限公司、福建省海峡信息技术有限公司、江苏晟晖信息科技有限公司、华泰证券股份有限公司、江苏金盾检测技术股份有限公司、联想集团、任子行网络技术股份有限公司、江苏天竞云合数据技术有限公司、山东鼎夏智能科技有限公司、山东云天安全技术有限公司、云南联创网安科技有限公司、河南灵创电子科技有限公司、内蒙古奥创网安科技有限公司、北京威努特技术有限公司、平安银河实验室、浙江大学 307LAB、赛尔网络有限公司、广西网信信息技术有限公司、北京固鸿科技有限公司、湖南轻山信息技术有限公司、福建中信网安信息科技有限公司、北京君云天下科技有限公司、合肥梆梆信息科技有限公司、北京微步在线科技有限公司、宁夏凯信特信息科技有限公司、安徽思珀特信息科技有限公司、苏州棱镜七彩信息科技有限公司、建信金科网络攻击实验室、中孚安全技术有限公司、福建奇比特信息科技有限公司、国网十堰供电公司信息通信分公司、杭州美创科技有限公司、贵州华黔信安信息技术有限公司、国网湖北省电力有限公司、广东唯顶信息科技股份有限公司、山东新潮信息技术有限公司、星云博创科技有限公司及其他个人白帽子向 CNVD 提交了 9435 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 5755 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）	3643	3643
奇安信网神（补天平台）	980	980
北京神州绿盟科技有限公司	782	8
上海交大	767	767
新华三技术有限公司	621	0
远江盛邦（北京）网络安全科技股份有限公司	583	583
厦门服云信息科技有限公司	544	0
北京启明星辰信息安全技术有限公司	420	9
三六零数字安全科技集团有限公司	365	365
深信服科技股份有限公司	354	4
北京天融信网络安全技术有限公司	285	19
安天科技集团股份有限公司	193	0
阿里云计算有限公司	180	3
天津市国瑞数码安全系统股份有限公司	118	0
杭州安恒信息技术股份有限公司	69	69
京东科技信息技术有限公司	40	3
北京数字观星科技有限公司	29	0
杭州迪普科技股份有限公司	17	3
中国电信集团系统集成有限责任公司	8	0

北京长亭科技有限公司	2	2
北京知道创宇信息技术股份有限公司	2	0
北京智游网安科技有限公司	1	1
快页信息技术有限公司	523	523
北京升鑫网络科技有限公司	127	127
北京山石网科信息技术有限公司	80	80
河南信安世纪科技有限公司	40	40
博智安全科技股份有限公司	31	31
安徽锋刃信息科技有限公司	18	18
河南东方云盾信息技术有限公司	12	12
福建省海峡信息技术有限公司	7	7
江苏晟晖信息科技有限公司	5	5
华泰证券股份有限公司	5	5
江苏金盾检测技术股份有限公司	5	5
联想集团	5	5
任子行网络技术股份有限公司	5	5
江苏天竞云合数据技术有限公司	4	4
山东鼎夏智能科技有限公司	4	4

山东云天安全技术有限公司	4	4
云南联创网安科技有限公司	3	3
河南灵创电子科技有限公司	3	3
内蒙古奥创网安科技有限公司	2	2
北京威努特技术有限公司	2	2
平安银河实验室	2	2
浙江大学 307LAB	2	2
赛尔网络有限公司	2	2
广西网信信息技术有限公司	2	2
北京固鸿科技有限公司	1	1
湖南轻山信息技术有限公司	1	1
福建中信网安信息科技有限公司	1	1
北京君云天下科技有限公司	1	1
合肥梆梆信息科技有限公司	1	1
北京微步在线科技有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
安徽思珀特信息科技有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
建信金科网络攻击实验室	1	1

中孚安全技术有限公司	1	1
福建奇比特信息科技有限公司	1	1
国网十堰供电公司信息通信分公司	1	1
杭州美创科技有限公司	1	1
贵州华黔信安信息技术有限公司	1	1
国网湖北省电力有限公司	1	1
广东唯顶信息科技股份有限公司	1	1
山东新潮信息技术有限公司	1	1
星云博创科技有限公司	1	1
亚信科技（成都）有限公司	1	0
北京华顺信安信息技术有限公司	1	0
CNCERT 广西分中心	7	7
CNCERT 贵州分中心	3	3
CNCERT 河北分中心	2	2
个人	2052	2052
报送总计	12981	9435

本周漏洞按类型和厂商统计

本周，CNVD 收录了 446 个漏洞。WEB 应用 290 个，应用程序 73 个，网络设备（交换机、路由器等网络端设备）52 个，操作系统 12 个，智能设备（物联网终端设备）10 个，安全产品 4 个，区块链 3 个，数据库 2 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	290
应用程序	73
网络设备（交换机、路由器等网络端设备）	52
操作系统	12
智能设备（物联网终端设备）	10
安全产品	4
区块链	3
数据库	2

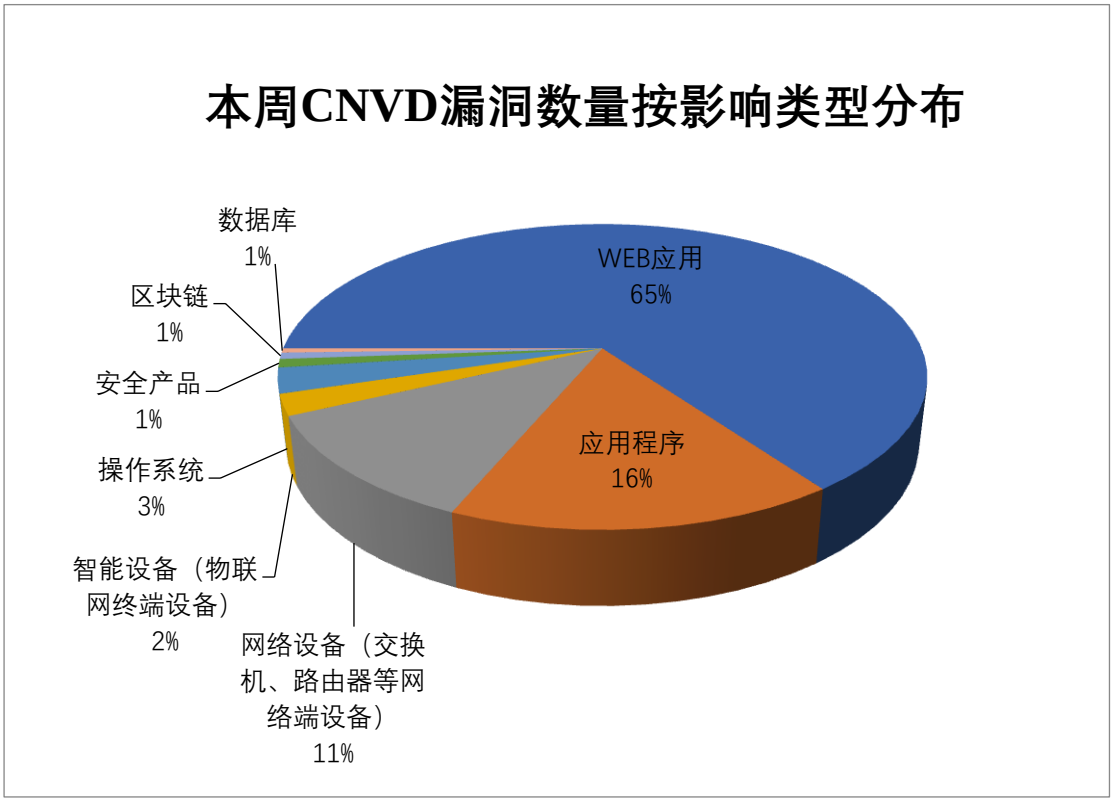

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Adobe、北京神州数码云科信息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	D-Link	16	4%
2	Adobe	13	3%
3	北京神州数码云科信息技术有限公司	13	3%
4	Apache	13	3%
5	Foxit	12	2%
6	Google	12	2%
7	北京百卓网络技术有限公	9	2%

	司		
8	Multi Language Pharmacy Management System	8	2%
9	Tenda	7	2%
10	其他	343	77%

本周行业漏洞收录情况

本周，CNVD 收录了 41 个电信行业漏洞，37 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-3040 缓冲区溢出漏洞、Google Android 权限提升漏洞（CNVD-2023-26074）”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/

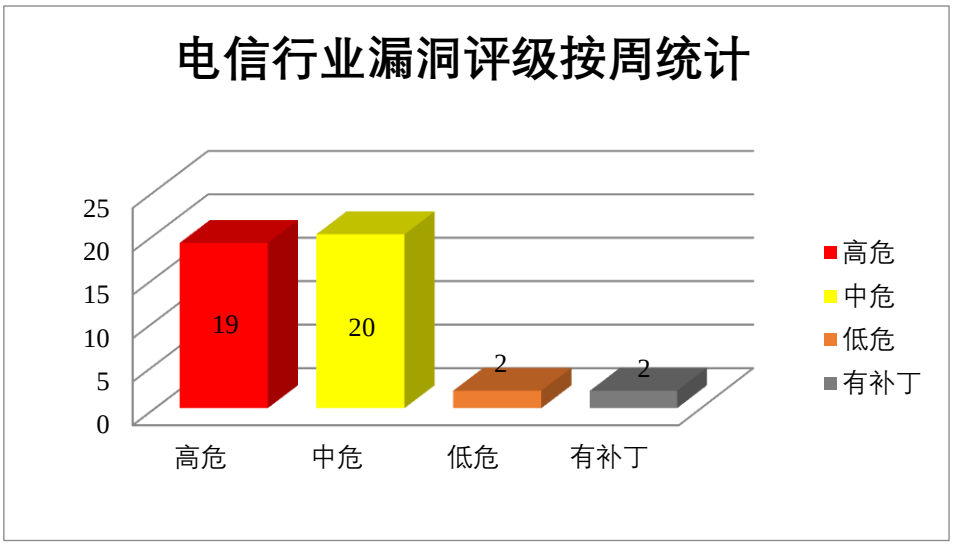

图 3 电信行业漏洞统计

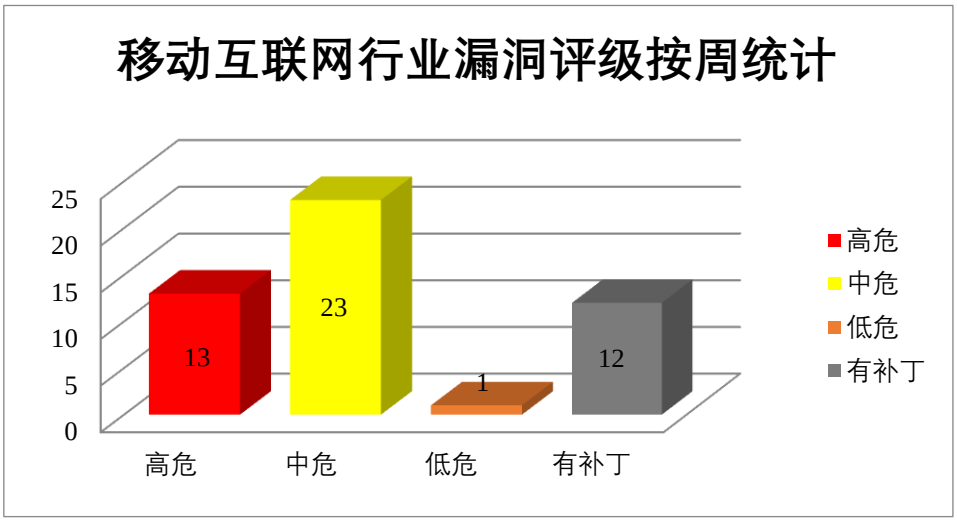

图 4 移动互联网行业漏洞统计

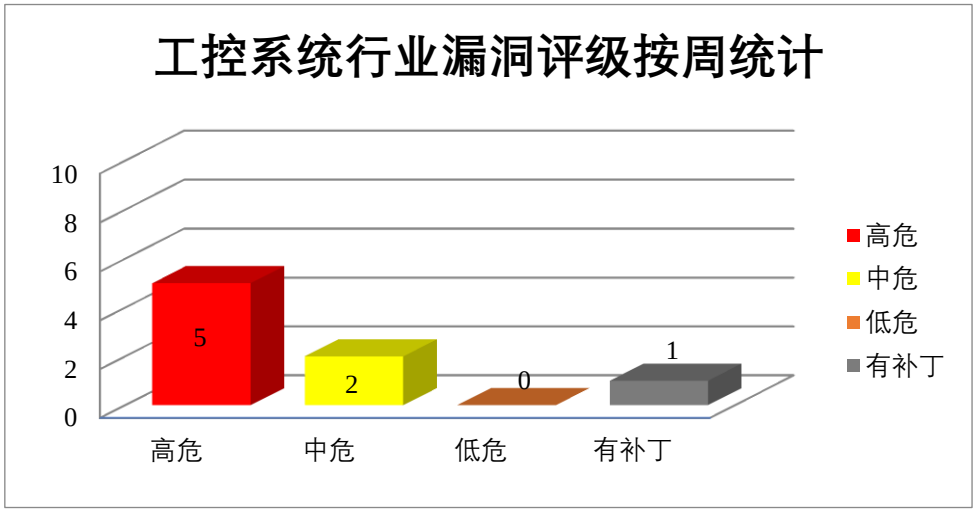

图 5 工控系统行业漏洞统计

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 Dimension 是美国奥多比（Adobe）公司的是一套 2D 和 3D 合成设计工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Dimension 越界读取漏洞（CNVD-2023-25103、CNVD-2023-25105、CNVD-2023-25106、CNVD-2023-27689）、Adobe Dimension 堆缓冲区溢出漏洞（CNVD-2023-25104、CNVD-2023-25109、CNVD-2023-25112、CNVD-2023-25111）。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-2023-25103

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25105

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25106

https://www.cnvd.org.cn/flaw/show/CNVD-2023-27689

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25104

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25109

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25112

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25111

2、 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。

CNVD 收录的相关漏洞包括：Google Android 越界读取漏洞（CNVD-2023-26065）、Google Android 信息泄露漏洞（CNVD-2023-26071）、Google Android 权限提升漏洞（CNVD-2023-26069、CNVD-2023-26070、CNVD-2023-26072、CNVD-2023-26073、CNVD-2023-26074、CNVD-2023-26078）。其中，除“Google Android 信息泄露漏洞（CNVD-2023-26071）、Google Android 权限提升漏洞（CNVD-2023-26078）”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-2023-26065

https://www.cnvd.org.cn/flaw/show/CNVD-2023-26071

https://www.cnvd.org.cn/flaw/show/CNVD-2023-26069

https://www.cnvd.org.cn/flaw/show/CNVD-2023-26070

https://www.cnvd.org.cn/flaw/show/CNVD-2023-26072

https://www.cnvd.org.cn/flaw/show/CNVD-2023-26073

https://www.cnvd.org.cn/flaw/show/CNVD-2023-26074

https://www.cnvd.org.cn/flaw/show/CNVD-2023-26078

3、 Apache 产品安全漏洞

Apache OpenOffice 是美国阿帕奇（Apache）基金会的一款开源的办公软件套件。该套件包含文本文档、电子表格、演示文稿、绘图、数据库等。Apache UIMA DUCC 是美国阿帕奇（Apache）基金会的一套集群管理系统。该系统提供工具，管理和调度工具。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。Apache Sling 是美国阿帕奇（Apache）基金会的一个 Java 平台的开源 Web 框架。旨在在符合 JSR-170 的内容存储库（例如 Apache Jackrabbi）上创建以内容为中心的应用程序。Apache Kerby 是美国阿帕奇（Apache）基金会的一个 Java Kerberos 绑定。提供了丰富、直观和可互操作的实现、库、KDC 和各种设施，可根据现代环境（如云、Hadoop 和移动）的需要集成 PKI、OTP 和令牌（OAuth2）。Apache Dubbo 是美国阿帕奇（Apache）

基金会的一款基 Jav 的轻量级 RPC（远程过程调用）框架。该产品提供了基于接口的远程呼叫、容错和负载平衡以及自动服务注册和发现等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码等。

CNVD 收录的相关漏洞包括：Apache OpenOffice 代码执行漏洞（CNVD-2023-25931）、Apache OpenOffice 代码问题漏洞、Apache UIMA DUCC 命令注入漏洞、Apache Sling JNDI 注入漏洞、Apache Kerby LDAP 注入漏洞、Apache Dubbo 代码问题漏洞（CNVD-2023-25935）、Apache InLong 反序列化漏洞（CNVD-2023-25936、CNVD-2023-25934）。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-2023-25931

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25930

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25928

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25934

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25933

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25932

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25935

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25936

4、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，攻击者可利用漏洞获取敏感信息，在当前进程的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2023-25114）、Foxit PDF Reader 资源管理错误漏洞（CNVD-2023-25118、CNVD-2023-25117、CNVD-2023-25116、CNVD-2023-25121、CNVD-2023-25120、CNVD-2023-25119、CNVD-2023-25122）。其中，除“Foxit PDF Reader 缓冲区溢出漏洞（CNVD-2023-25114）”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-2023-25114

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25118

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25117

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25116

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25121

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25120

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25119

https://www.cnvd.org.cn/flaw/show/CNVD-2023-25122

5、D-Link DIR-846 命令执行漏洞（CNVD-2023-27681）

D-Link DIR-846 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-846 被披露存在命令执行漏洞，攻击者可利用该漏洞在系统上执行任意命令。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-2023-27681

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-2023-25102	ICONICS GENESIS64 路径遍历漏洞	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.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-008_en.pdf
CNVD-2023-25107	Adobe Dimension 内存错误引用漏洞（CNVD-2023-25107）	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/dimension/apsb23-20.html
CNVD-2023-25929	Apache Fineract 服务器请求伪造漏洞	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://lists.apache.org/thread/m58fdjmtkfp9h4c0r4l48rv995w3qhb6
CNVD-2023-26064	Google Android 权限提升漏洞（CNVD-2023-26064）	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/docs/security/bulletin/pixel/2022-12-01
CNVD-2023-27674	D-Link DIR-3040 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10322
CNVD-2023-27690	Adobe Dimension 不当输入验证漏洞	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/dimension/apsb23-20.html
CNVD-2023-26067	Google Android 权限提升漏洞（CNVD-2023-26067）	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/2023-02-01
CNVD-2023	Adobe Dimension 内存错误	高	厂商已发布了漏洞修复程序，请及

-25110	引用漏洞（CNVD-2023-25110）		时关注更新：https://helpx.adobe.com/security/products/dimension/apsb23-20.html
CNVD-2023-26066	Google Android 权限提升漏洞（CNVD-2023-26066）	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/2023-02-01
CNVD-2023-25108	Adobe Dimension 内存错误引用漏洞（CNVD-2023-25108）	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/dimension/apsb23-20.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Google、Apache、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，提升权限，执行任意代码等。另外，D-Link DIR-846 被披露存在命令执行漏洞，攻击者可利用该漏洞在系统上执行任意命令。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 RX9 Pro setIPv6Status 缓冲区溢出漏洞

验证描述

Tenda RX9 Pro 是中国腾达（Tenda）公司的一款无线路由器。

Tenda RX9 Pro 存在缓冲区溢出漏洞，该漏洞源于 setIPv6Status 对于输入的数据缺乏长度检查，攻击者可利用漏洞导致代码执行或者拒绝服务。

验证信息

POC 链接：https://github.com/whiter6666/CVE/blob/main/Tenda_RX9_Pro/setIPv6Status.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-27632

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. 微软 Azure 曝“设计缺陷”，暴露存储账户

The Hacker News 网站披露，研究人员发现微软 Azure 中存在一个“设计缺陷”，一旦攻击者成功利用，便可以访问存储帐户，甚至可在内部系统环境中横向移动，执行远程代码。

参考链接：https://www.freebuf.com/news/363318.html

2. vm2 JavaScript 沙箱存在安全漏洞

vm2 JavaScript 沙箱模块背后的开发人员已经解决了一个安全漏洞，跟踪为 CVE-2023-29017（CVSS 评分 9.8），该漏洞可被利用来执行任意 shellcode。

参考链接：https://blog.wuhao13.xin/5576.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