国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 07 月 29 日-2024 年 08 月 04 日 **2024 年第 31 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 410 个，其中高危漏洞 215 个、中危漏洞 177 个、低危漏洞 18 个。漏洞平均分值为 6.64。本周收录的漏洞中，涉及 0day 漏洞 261 个（占 64%），其中互联网上出现“Tenda AC 10 缓冲区溢出漏洞（CNVD-2024-34381）、Cesanta MJS 拒绝服务漏洞（CNVD-2024-34384）”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 45205 个，与上周（54241）环比减少 17%。

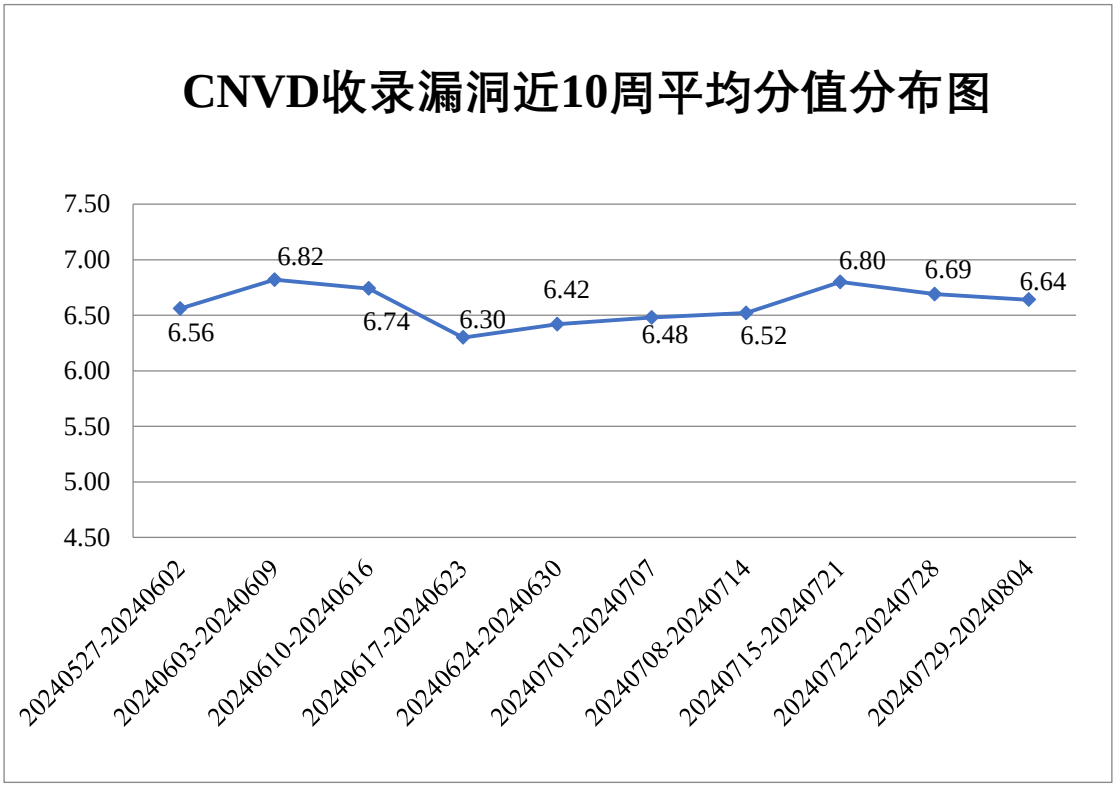

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 2 起，向基础电信企业通报漏洞事件 4 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 337 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 30 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 6 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：

紫光软件系统有限公司、中控技术股份有限公司、中犇科技有限公司、智互联（深圳）科技有限公司、浙江大华技术股份有限公司、长春市本源经贸有限公司、漳州豆壳网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、夏普商贸（中国）有限公司、武汉达梦数据库股份有限公司、威海轩辕计算机科技有限公司、威步信息系统（上海）有限公司、天津市天科数创科技股份有限公司、台达电子企业管理（上海）有限公司、苏州真趣信息科技有限公司、苏州科达科技股份有限公司、深圳市锐明技术股份有限公司、深圳市蓝凌软件股份有限公司、深圳市金蝶妙想互联有限公司、深圳市吉祥腾达科技有限公司、深圳市富士智能系统有限公司、深圳市顶讯网络科技有限公司、深圳市道尔智控科技股份有限公司、上海锐昉科技有限公司、上海肯特仪表股份有限公司、上海寰创通信科技股份有限公司、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、山东山大华天软件有限公司、山东比特智能科技股份有限公司、厦门科拓通讯技术股份有限公司、三星（中国）投资有限公司、赛蓝（广州）信息技术有限公司、任子行网络技术股份有限公司、青岛和正信息技术有限公司、南通润邦网络科技有限公司、南昌蓝智科技有限公司、灵宝简好网络科技有限公司、浪潮集团有限公司、京瓷办公信息系统（中国）有限公司、佳能（中国）有限公司、济南爱程网络科技有限公司、吉翁电子（深圳）有限公司、华平信息技术股份有限公司、红火蚁科技有限公司、恒生电子股份有限公司、河北南昊高新技术开发有限公司、杭州雄伟科技开发股份有限公司、杭州荷花软件有限公司、杭州禾诺信息技术有限公司、杭州安恒信息技术股份有限公司、哈尔滨新中新电子股份有限公司、广州图创计算机软件开发有限公司、飞救医疗科技（北京）有限公司、泛微网络科技股份有限公司、鼎捷软件股份有限公司、大连大有吴涛易语言软件开发有限公司、创业慧康科技股份有限公司、成都卓越远扬信息技术有限公司、成都天问互联科技有限公司、成都索贝数码科技股份有限公司、成都生动网络科技有限公司、畅捷通信息技术股份有限公司、北京中科商软软件有限公司、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、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京通王科技有限公司、北京神州视翰科技有限公司、北京人大金仓信息技术股份有限公司、北京平凯星辰科技发展有限公司、北京金盘鹏图软件技术有限公司、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、北大医疗信息技术有限公司、奥琦玮信息科技（北京）有限

公司、安科瑞电气股份有限公司和艾锐势科技（深圳）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，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、北京天融信网络安全技术有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。江苏金盾检测技术股份有限公司、江苏云天网络安全技术有限公司、北京翰慧投资咨询有限公司、河南东方云盾信息技术有限公司、成都久信信息技术股份有限公司、江西中和证信息安全技术有限公司、快页信息技术有限公司、中资网络信息安全科技有限公司、重庆都会信息科技有限公司、星云博创科技有限公司、南方电网数字电网集团信息通信科技有限公司、苏州棱镜七彩信息科技有限公司、中国科学院计算机网络信息中心、成都安美勤信息技术股份有限公司、软通动力信息技术（集团）股份有限公司、江苏极元信息技术有限公司、北京安华金和科技有限公司、上海直画科技有限公司、河南宝通信息安全测评有限公司、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、国家计算机病毒应急处理中心、杭州孝道科技有限公司、上海只柏特信息技术有限公司、广州华南检验检测中心有限公司、上海恒岳安全技术服务有限公司、上海观安信息技术股份有限公司、国网宁夏电力有限公司石嘴山供电公司、北京威努特技术有限公司、江苏正信信息安全测试有限公司、国网江西省电力有限公司电力科学研究院、福建浩程信息科技有限公司、湖南泛联新安信息科技有限公司、亚信科技（成都）有限公司及其他个人白帽子向 CNVD 提交了 45205 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 43915 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	原创漏洞数量
斗象科技（漏洞盒子）	25004	25004
奇安信网神（补天平台）	16535	16535
三六零数字安全科技集团有限公司	2232	2232
新华三技术有限公司	713	0
安天科技集团股份有限公司	460	0
深信服科技股份有限公司	301	0

北京天融信网络安全技术有限公司	256	14
阿里云计算有限公司	166	6
上海交大	144	144
杭州安恒信息技术股份有限公司	83	58
恒安嘉新（北京）科技股份公司	83	0
北京启明星辰信息安全技术有限公司	72	3
北京安信天行科技有限公司	41	41
北京长亭科技有限公司	33	0
杭州迪普科技股份有限公司	30	0
京东科技信息技术有限公司	23	0
北京知道创宇信息技术有限公司	19	0
中国电信集团系统集成有限责任公司	10	10
西安四叶草信息技术有限公司	6	6
远江盛邦（北京）网络安全科技股份有限公司	6	6
内蒙古奥创科技有限公司	3	3
北京智游网安科技有限公司	2	2
华为技术有限公司	1	1
贵州泰若数字科技有限公司	1	1
江苏金盾检测技术股	59	59

份有限公司		
江苏云天网络安全技术有限公司	43	43
北京翰慧投资咨询有限公司	17	17
河南东方云盾信息技术有限公司	16	16
成都久信信息技术股份有限公司	13	13
江西中和证信息安全技术有限公司	12	12
快页信息技术有限公司	11	11
中资网络信息安全科技有限公司	7	7
重庆都会信息科技有限公司	5	5
星云博创科技有限公司	5	5
南方电网数字电网集团信息通信科技有限公司	4	4
苏州棱镜七彩信息科技有限公司	4	4
中国科学院计算机网络信息中心	3	3
成都安美勤信息技术股份有限公司	3	3
软通动力信息技术（集团）股份有限公司	3	3
江苏极元信息技术有限公司	3	3
亚信科技（成都）有限公司	2	2

北京安华金和科技有限公司	2	2
上海直画科技有限公司	2	2
河南宝通信息安全测评有限公司	2	2
北京卓识网安技术股份有限公司	1	1
安徽天行网安信息安全技术有限公司	1	1
国家计算机病毒应急处理中心	1	1
杭州孝道科技有限公司	1	1
上海只柏特信息技术有限公司	1	1
广州华南检验检测中心有限公司	1	1
上海恒岳安全技术服务有限公司	1	1
上海观安信息技术股份有限公司	1	1
国网宁夏电力有限公司石嘴山供电公司	1	1
北京威努特技术有限公司	1	1
江苏正信信息安全测试有限公司	1	1
国网江西省电力有限公司电力科学研究院	1	1
福建浩程信息科技有限公司	1	1
湖南泛联新安信息科技有限公司	1	1
CNCERT 宁夏分中心	6	6

个人	903	903
报送总计	47363	45205

本周漏洞按类型和厂商统计

本周，CNVD 收录了 410 个漏洞。WEB 应用 156 个，应用程序 120 个，网络设备（交换机、路由器等网络端设备）93 个，操作系统 18 个，智能设备（物联网终端设备）18 个，安全产品 3 个，数据库 1 个，车联网 1 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	156
应用程序	120
网络设备（交换机、路由器等网络端设备）	93
操作系统	18
智能设备（物联网终端设备）	18
安全产品	3
数据库	1
车联网	1

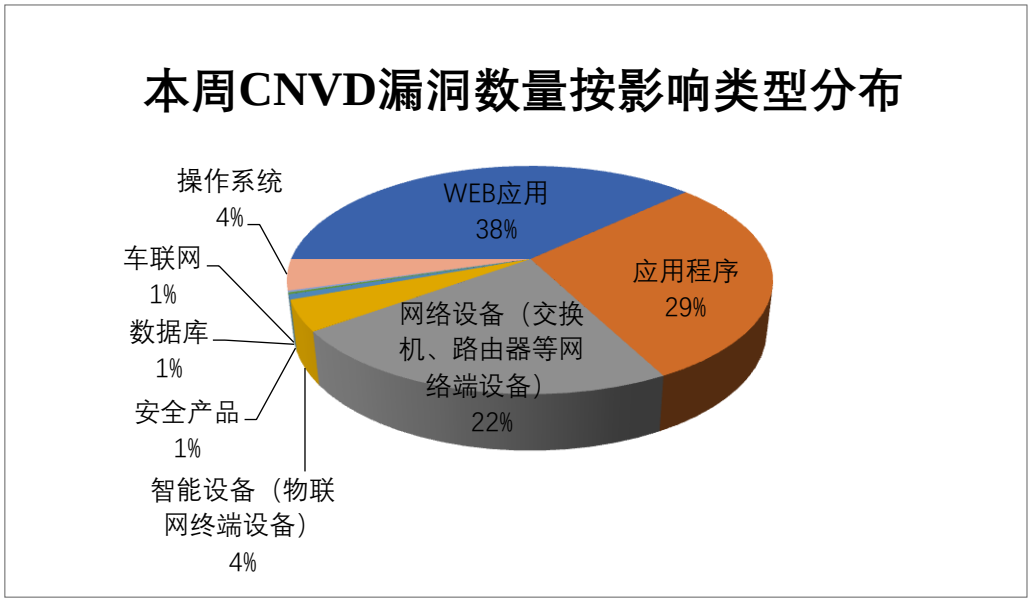

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Splunk、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	5%

2	Splunk	15	4%
3	Foxit	15	4%
4	LG	14	3%
5	Huawei	14	3%
6	北京星网锐捷网络技术有限公司	13	3%
7	D-Link	13	3%
8	深圳市吉祥腾达科技有限公司	12	3%
9	Jungo Connectivity	12	3%
10	其他	281	69%

本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，20 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“SyroTech SY-GPON-1110-WDONT 信息泄露漏洞、Huawei HarmonyOS 和 EMUI AMS 模块拒绝服务漏洞”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/

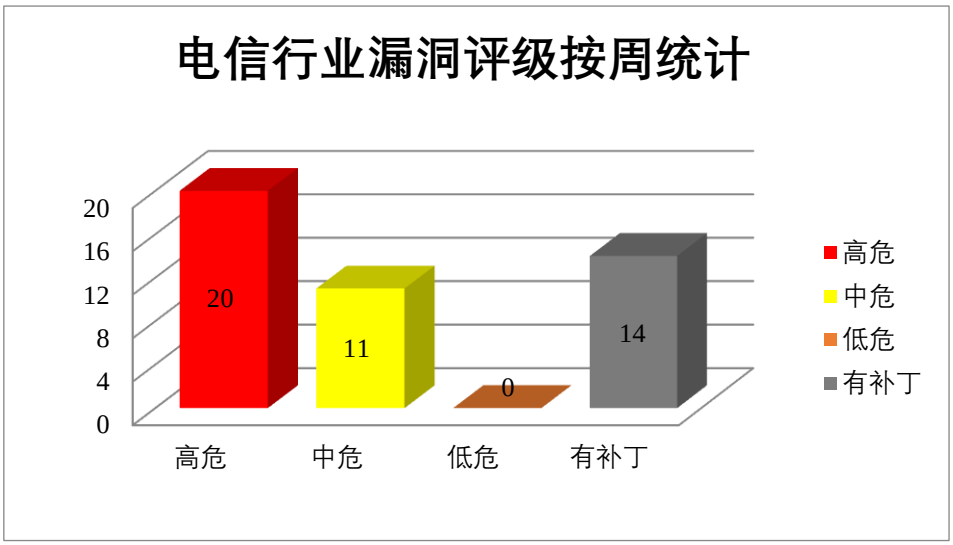

图 3 电信行业漏洞统计

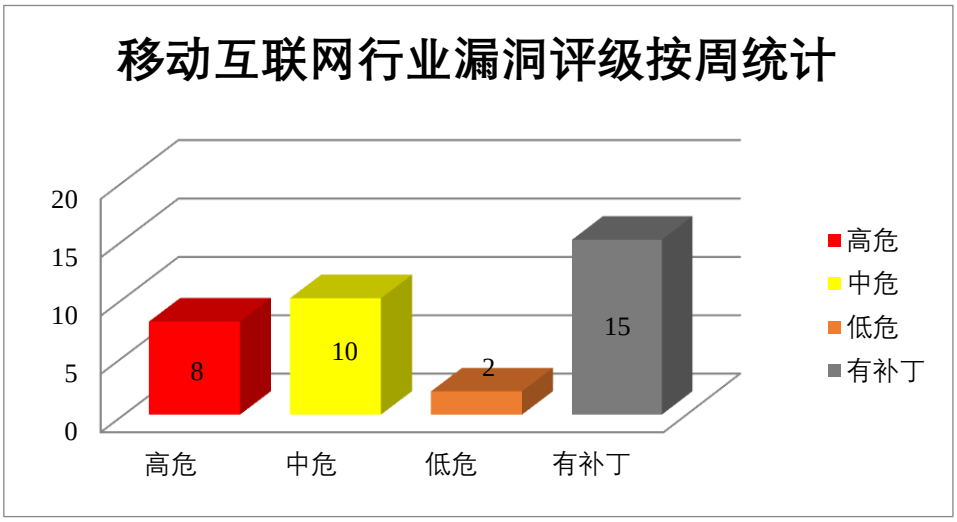

图 4 移动互联网行业漏洞统计

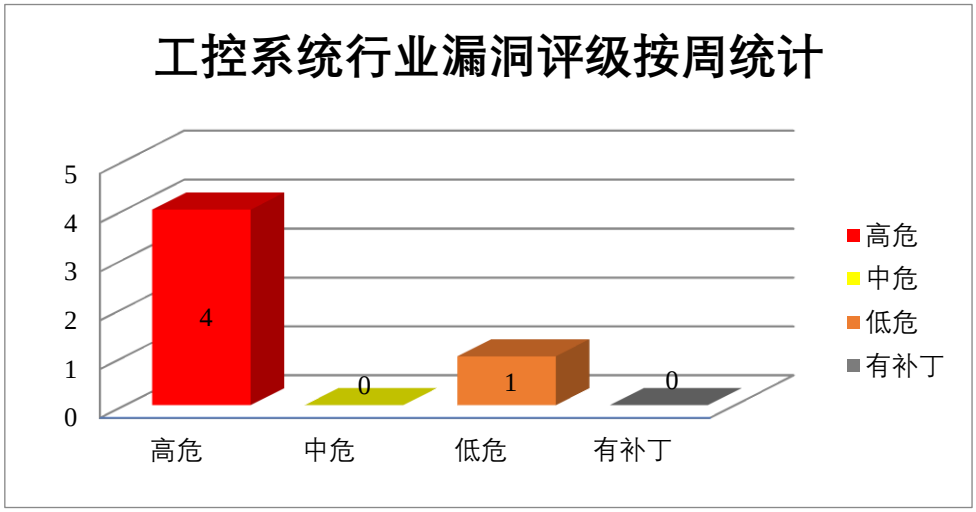

图 5 工控系统行业漏洞统计

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、 Apache 产品安全漏洞

Apache Arrow 是美国阿帕奇（Apache）基金会的一款用于内存数据处理的跨语言开发平台。该平台支持 C、C++、C＃、Go 和 Java 等编程语言，并提供进程间通信等功能。Apache CloudStack 是美国阿帕奇（Apache）基金会的一套基础架构即服务（IaaS）云计算平台。该平台主要用于部署和管理大型虚拟机网络。Apache CXF 是美国阿帕奇（Apache）基金会的一个开源的 Web 服务框架。该框架支持多种 Web 服务标准、多种前端编程 API 等。Apache RocketMQ 是美国阿帕奇（Apache）基金会的一款轻量级的数据处理平台和消息传递引擎。Apache StreamPark 是美国阿帕奇（Apache）基金会的一个流媒体应用程序开发框架。Apache HTTP Server 是美国阿帕奇（Apache）基金会

的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞使用授权令牌手动发出请求，获取敏感信息，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Apache Arrow Rust Object Store 日志信息泄露漏洞、Apache CloudStack 安全绕过漏洞（CNVD-2024-33812）、Apache CXF 内存消耗漏洞、Apache RocketMQ 信息泄露漏洞、Apache StreamPark 权限管理错误漏洞、Apache HTTP Server 信息泄露漏洞（CNVD-2024-33815）、Apache HTTP Server 服务器端请求伪造漏洞、Apache StreamPark 信息泄露漏洞。其中，“Apache CloudStack 安全绕过漏洞（CNVD-2024-33812）、Apache CXF 内存消耗漏洞”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-2024-33806
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33812
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33811
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33810
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33809
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33815
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33814
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33813

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，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 内存错误引用漏洞（CNVD-2024-33836、CNVD-2024-33835、CNVD-2024-33839、CNVD-2024-33837、CNVD-2024-33843、CNVD-2024-33841）、Foxit PDF Reader 越界读取漏洞（CNVD-2024-33838）、Foxit PDF Reader 越界写入漏洞（CNVD-2024-33840）。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-2024-33836
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33835
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33839
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33838
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33837
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33843
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33841

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33840

3、Microsoft 产品安全漏洞

Microsoft Outlook 是美国微软（Microsoft）公司的一套电子邮件应用程序。Microsoft Dynamics 365 是美国微软（Microsoft）公司的一套适用于跨国企业的 ERP 业务解决方案。该产品包括财务管理、生产管理和商业智能管理等。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞进行欺骗攻击，获取敏感信息，提升权限，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Outlook 远程代码执行漏洞（CNVD-2024-34105）、Microsoft Outlook 欺骗漏洞（CNVD-2024-34107）、Microsoft Outlook for Android 信息泄露漏洞、Microsoft Outlook 权限提升漏洞（CNVD-2024-34109）、Microsoft Outlook 远程代码执行漏洞（CNVD-2024-34111）、Microsoft Dynamics 365 (on-premises)信息泄露漏洞（CNVD-2024-34112）、Microsoft Dynamics 365 Business Central 权限提升漏洞、Microsoft Dynamics 365 Business Central 远程代码执行漏洞（CNVD-2024-34114）。其中，除“Microsoft Outlook 权限提升漏洞（CNVD-2024-34109）”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-2024-34105

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34107

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34108

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34109

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34111

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34112

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34113

https://www.cnvd.org.cn/flaw/show/CNVD-2024-34114

4、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 InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。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 Acrobat 是美国奥多比（Adobe）公司的一套 PDF 文件编辑和转换工具。Adobe ColdFusion 是美国奥多比（Adobe）公司的一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问受限目录之外的文件和目录，并覆盖任意文件，在系统上执行任意代码或导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Adobe Bridge 越界读取漏洞（CNVD-2024-34085）、Adobe InDesign 堆缓冲区溢出漏洞（CNVD-2024-34087、CNVD-2024-34088、CNVD-2024-34093）、Adobe InDesign 越界写入漏洞（CNVD-2024-34089）、Adobe Premiere

Pro 不受信任搜索路径漏洞、Adobe Acrobat Android 路径遍历漏洞、Adobe ColdFusion 访问控制错误漏洞（CNVD-2024-34094）。其中，除“Adobe Bridge 越界读取漏洞（CNVD-2024-34085）、Adobe Premiere Pro 不受信任搜索路径漏洞、Adobe Acrobat Android 路径遍历漏洞”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-2024-34085
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34087
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34088
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34089
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34090
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34092
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34093
https://www.cnvd.org.cn/flaw/show/CNVD-2024-34094

5、LG Simple Editor 拒绝服务漏洞

LG Simple Editor 是韩国乐金（LG）公司的一个简易编辑器，通过简化流程和在标牌上即时播放来创建新内容。本周，LG Simple Editor 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务。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-2024-34031

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-2024-33807	Apache Drill XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/9tt0q4bdjwgw0dz0l9knqxjnpb5y6zsl
CNVD-2024-33897	NETGEAR ProSAFE 任意文件上传漏洞（CNVD-2024-33897）	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://kb.netgear.com/000065707/Security-Advisory-for-Multiple-Vulnerabilities-on-the-ProSAFE-Network-Management-System-PSV-2023-0024-PSV-2023-0025
CNVD-2024-33896	D-Link DAP-1325 命令注入漏洞（CNVD-2024-33896）	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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10351
CNVD-2024-33902	NETGEAR ProSAFE 目录遍历漏洞	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://kb.netgear.com/000065705/Security-Advisory-for-Post-authentication-Command-Injection-on-the-Prosafe-Network-Management-System-PSV-2023-0037
CNVD-2024-33901	D-Link DAP-1325 栈缓冲区溢出漏洞（CNVD-2024-33901）	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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10351
CNVD-2024-34082	Kofax Power PDF 远程代码执行漏洞	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://www.kofax.com/products/power-pdf/
CNVD-2024-34273	Splunk Enterprise 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://advisory.splunk.com/advisories/SVD-2024-0711
CNVD-2024-34375	SyroTech SY-GPON-1110-WDONT 信息泄露漏洞（CNVD-2024-34375）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.syrotech.com/product-page/sy-gpon-1101-wdont
CNVD-2024-34390	Huawei HarmonyOS 和 EMUI 锁屏模块权限校验类漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/en/support/bulletin/2024/4/ https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202404-0000001880501689
CNVD-2024-34393	Huawei HarmonyOS 和 EMUI 拒绝服务漏洞（CNVD-2024-34393）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/en/support/bulletin/2024/4/

小结：本周，Apache 产品被披露存在多个漏洞，攻击者可利用漏洞使用授权令牌

手动发出请求，获取敏感信息，导致拒绝服务等。此外，Foxit、Microsoft、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，获取敏感信息，覆盖任意文件，提升权限，在系统上执行任意代码或导致应用程序崩溃等。另外，LG Simple Editor 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务。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、Tenda AC10 缓冲区溢出漏洞（CNVD-2024-34381）

验证描述

Tenda AC10 是中国腾达（Tenda）公司的一款无线路由器。

Tenda AC10 存在缓冲区溢出漏洞，该漏洞源于文件/goform/SetStaticRouteCfg 的 fromSetRouteStatic 函数的参数 list 未能正确验证输入数据的长度大小，攻击者可利用该漏洞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/abcdefg-png/IoT-vulnerable/blob/main/Tenda/AC10/V16.03.10.13/fromSetRouteStatic.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-34381

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. 苹果修复了 iOS 和 macOS 中的多个安全漏洞

Apple 发布了安全性更新，以应对 iOS、macOS、tvOS、visionOS、watchOS 和 Safari 中的多个安全漏洞。

Apple 公司发布了 iOS 17.6 和 iPadOS 17.6 以解决多个安全漏洞。

参考链接：https://securityaffairs.com/166390/mobile-2/apple-ios-17-6-and-ipados-17-6.html

2. 攻击者劫持 Facebook 页面用于推广恶意 AI 照片编辑器

近日，有攻击者劫持了 Facebook 上的网页，诱骗用户下载一个合法的人工智能（A

I）照片编辑器，但实际上他们真正下载的却是一个专门用以盗取用户的凭据信息窃取程序。

参考链接：https://www.freebuf.com/news/407579.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