

## 信息安全漏洞周报

2024年12月23日-2024年12月29日

2024年第52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 303 个，其中高危漏洞 167 个、中危漏洞 119 个、低危漏洞 17 个。漏洞平均分为 6.80。本周收录的漏洞中，涉及 0day 漏洞 214 个（占 71%），其中互联网上出现“TOTOLINK AC1200 setWizardCfg 函数缓冲区溢出漏洞、TOTOLINK AC1200 setWiFiRepeater Cfg 方法 password 参数缓冲区溢出漏洞”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 29176 个，与上周（36345 个）环比减少 20%。

### CNVD收录漏洞近10周平均分分布图

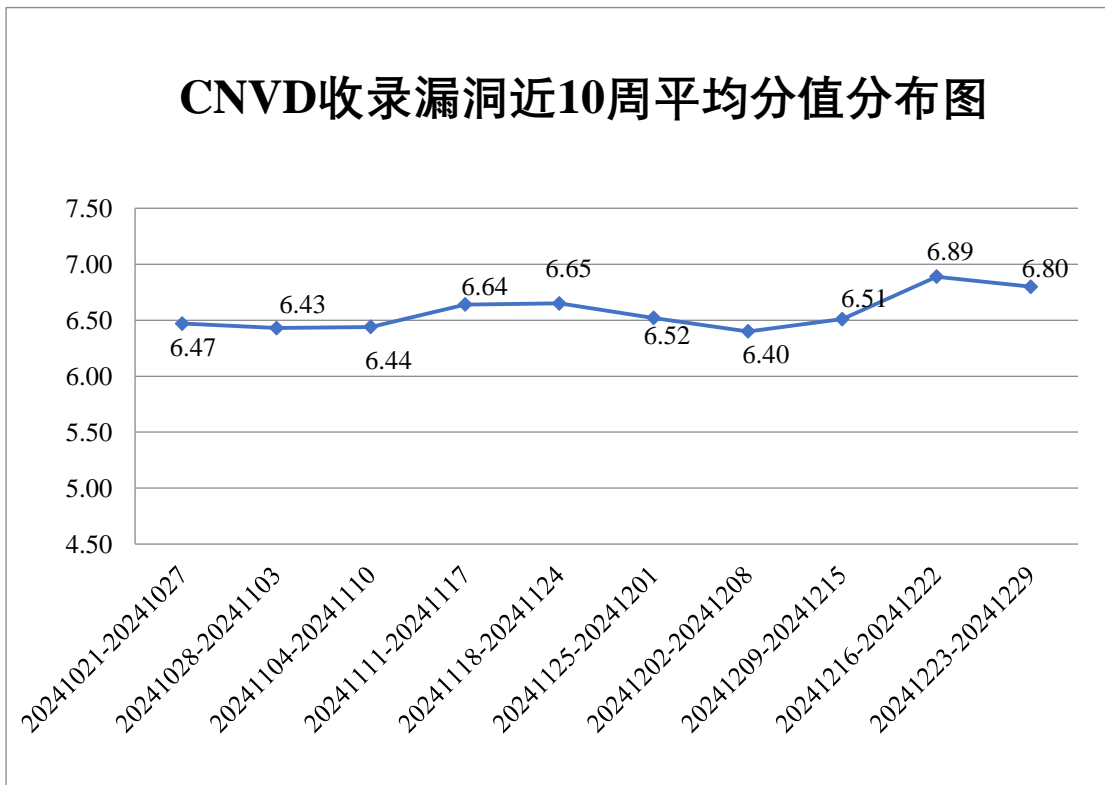



图 1 CNVD 收录漏洞近 10 周平均分分布图

### 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 6 起，向基础电信企业通报漏洞事件 2 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 654 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 53 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 23 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硬件产品存在的漏洞，具体处置单位情况如下所示：

上海捷煜智能科技有限公司、青岛海信网络科技股份有限公司、上海鹰谷信息科技有限公司、深圳拓安信物联股份有限公司、北京九思协同软件有限公司、软联科技（湖北）有限公司、北京数影互联科技有限公司、麦克奥迪实业集团有限公司、深圳市吉祥腾达科技有限公司、荣耀终端有限公司、广东保伦电子股份有限公司、用友网络科技股份有限公司、上海上讯信息技术股份有限公司、苏州德启智能科技有限公司、畅捷通信息技术股份有限公司、腾讯安全应急响应中心、吉翁电子（深圳）有限公司、广西南宁有爱科技有限公司、厦门四信通信科技有限公司、申瓯通信设备有限公司、网是科技股份有限公司、浙江大华技术股份有限公司、北京小桔科技有限公司、杭州叙简科技股份有限公司、科亚医疗科技股份有限公司、北京中庆现代技术股份有限公司、友讯电子设备（上海）有限公司、北京神州数码云科信息技术有限公司、西安众邦网络科技有限公司、泛微网络科技股份有限公司、苏州欧信达信息科技有限公司、武汉天地伟业科技有限公司、深圳市网旭科技有限公司、南昌卓蓝科技有限公司、深圳市磊科实业有限公司、京宏业汇成科技有限公司、北京神州视翰科技有限公司、北京仁和汇智信息技术有限公司、广州赛意信息科技股份有限公司、贵阳思普信息技术有限公司、望海康信（北京）科技股份公司、杭州新视窗信息技术有限公司、广州华壹智能科技有限公司、安科瑞电气股份有限公司、厦门福龙诚信息科技有限公司、西安华谊云信息科技有限公司、北京和欣运达科技有限公司、华平信息技术股份有限公司、山东比特智能科技股份有限公司、中电科金仓（北京）科技股份有限公司、紫光股份有限公司、北京宝兰德软件股份有限公司、北京惠朗时代科技有限公司、北京金和网络股份有限公司、北京通达信科科技有限公司、北京亚控科技发展有限公司、大连华天软件有限公司、广联达科技股份有限公司、广州红帆科技有限公司、熵基科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市企企通科技有限公司和深圳市思迅软件股份有限公司。



## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、北京数字观星科技有限公司、深信服科技股份有限公司、新华三技术有限公司、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。北京纽盾网安信息技术有限公司、成

都卫士通信息安全技术有限公司、江苏云天网络安全技术有限公司、北京山石网科信息技术有限公司、成都久信信息技术股份有限公司、淮安易云科技有限公司、北京时代新威信息技术有限公司、贵州多彩网安科技有限公司、江苏正信信息安全测试有限公司、北京翰慧投资咨询有限公司、北京天下信安技术有限公司、苏州棱镜七彩信息科技有限公司、北京安帝科技有限公司、博智安全科技股份有限公司、北京众安天下科技有限公司、北京远禾科技有限公司、福建省海峡信息技术有限公司、上海谋乐网络科技有限公司、北京安华金和科技有限公司、北京国信城研科学技术研究院、山东新潮信息技术有限公司、中电福富信息科技有限公司、江苏百达智慧网络科技有限公司(含光实验室)、中资网络信息安全科技有限公司、浙江大学控制科学与工程学院、山东正中信息技术股份有限公司、江苏锋刃信息科技有限公司、江苏保旺达软件技术有限公司、星云博创科技有限公司、哈尔滨理工大学信息安全与智能技术研究中心、中孚安全技术有限公司、北京微步在线科技有限公司、西安交大捷普网络科技有限公司、陕西青山四纪信息技术有限公司、御维网络安全技术有限公司、上海吨吨信息技术有限公司、信息产业信息安全测评中心、上海观安信息技术股份有限公司、湖南红点安全信息技术有限公司、河南东方云盾信息技术有限公司、湖北星野科技发展有限公司及其他个人白帽子向 CNVD 提交了 29176 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)、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 28059 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)	27130	27130
北京启明星辰信息安全技术有限公司	1525	7
三六零数字安全科技集团有限公司	787	787
北京数字观星科技有限公司	649	0
深信服科技股份有限公司	633	7
新华三技术有限公司	509	0
北京神州绿盟科技有限公司	395	0
安天科技集团股份有限公司	350	0
北京天融信网络安全	261	41

技术有限公司		
上海交大	142	142
南京众智维信息科技有限公司	132	10
杭州安恒信息技术股份有限公司	113	20
北京安信天行科技有限公司	85	85
中国电信集团系统集成有限责任公司	81	0
北京长亭科技有限公司	46	9
北京知道创宇信息技术有限公司	48	3
杭州迪普科技股份有限公司	11	1
京东科技信息技术有限公司	8	8
阿里云计算有限公司	6	6
杭州美创科技股份有限公司	5	5
华为技术有限公司	4	4
浪潮电子信息产业股份有限公司	2	2
深圳市腾讯计算机系统有限公司（玄武实验室）	2	2
快页信息技术有限公司	1	1
北京升鑫网络科技有限公司（青藤云安全）	1	1
北京纽盾网安信息技术有限公司	23	23
成都卫士通信息安全技术有限公司	18	18

江苏云天网络安全技术有限公司	11	11
北京山石网科信息技术有限公司	10	10
成都久信信息技术股份有限公司	9	9
淮安易云科技有限公司	7	7
北京时代新威信息技术有限公司	7	7
贵州多彩网安科技有限公司	6	6
江苏正信信息安全测试有限公司	5	5
北京翰慧投资咨询有限公司	5	5
北京天下信安技术有限公司	4	4
苏州棱镜七彩信息科技有限公司	4	4
北京安帝科技有限公司	3	3
博智安全科技股份有限公司	3	3
北京众安天下科技有限公司	3	3
北京远禾科技有限公司	2	2
福建省海峡信息技术有限公司	2	2
上海谋乐网络科技有限公司	2	2
北京安华金和科技有限公司	2	2
北京国信城研科学技	2	2

术研究院		
山东新潮信息技术有限公司	2	2
中电福富信息科技有限公司	2	2
江苏百达智慧网络科技有限公司（含光实验室）	2	2
中资网络信息安全科技有限公司	2	2
浙江大学控制科学与工程学院	2	2
山东正中信息技术股份有限公司	2	2
江苏锋刃信息科技有限公司	1	1
江苏保旺达软件技术有限公司	1	1
星云博创科技有限公司	1	1
哈尔滨理工大学信息安全与智能技术研究中心	1	1
中孚安全技术有限公司	1	1
北京微步在线科技有限公司	1	1
西安交大捷普网络科技有限公司	1	1
陕西青山四纪信息技术有限公司	1	1
御维网络安全技术有限公司	1	1
上海吨吨信息技术有限公司	1	1

信息产业信息安全测评中心	1	1
上海观安信息技术股份有限公司	1	1
湖南红点安全信息技术有限公司	1	1
河南东方云盾信息技术有限公司	1	1
湖北星野科技发展有限公司	1	1
CNCERT 宁夏分中心	2	2
CNCERT 河南分中心	2	2
CNCERT 贵州分中心	1	1
个人	745	745
报送总计	33831	29176

### 本周漏洞按类型和厂商统计

本周，CNVD 收录了 303 个漏洞。WEB 应用 178 个，应用程序 50 个，网络设备（交换机、路由器等网络端设备）38 个，操作系统 18 个，安全产品 11 个，智能设备（物联网终端设备）4 个，数据库 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	178
应用程序	50
网络设备（交换机、路由器等网络端设备）	38
操作系统	18
安全产品	11
智能设备（物联网终端设备）	4
数据库	4

## 本周CNVD漏洞数量按影响类型分布

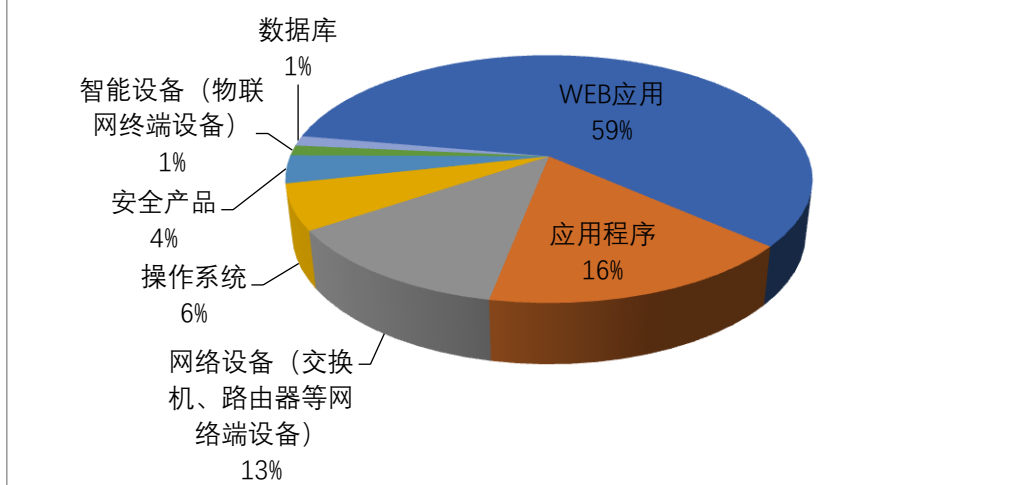


图2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、用友网络科技股份有限公司、青岛东胜伟业软件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	Adobe	20	6%
2	用友网络科技股份有限公司	12	4%
3	青岛东胜伟业软件有限公司	12	4%
4	IBM	11	4%
5	D-Link	11	4%
6	Google	10	3%
7	Apache	8	3%
8	北京神州视翰科技有限公司	8	3%
9	北京金和网络股份有限公司	7	2%
10	其他	204	67%

### 本周行业漏洞收录情况

本周，CNVD 收录了 19 个电信行业漏洞，8 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2024-49502）、Rockwell Automation Power Monitor 1000 设备接管漏洞”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/>

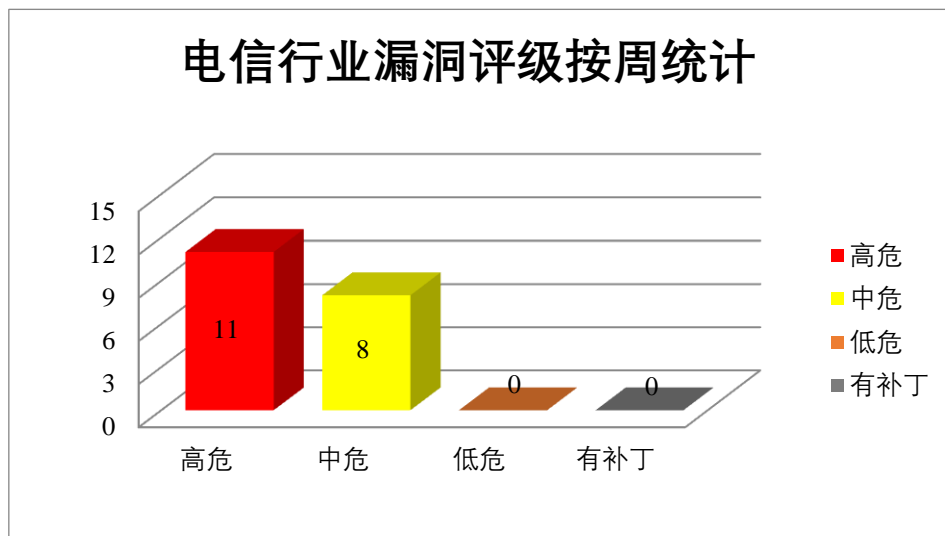


图 3 电信行业漏洞统计

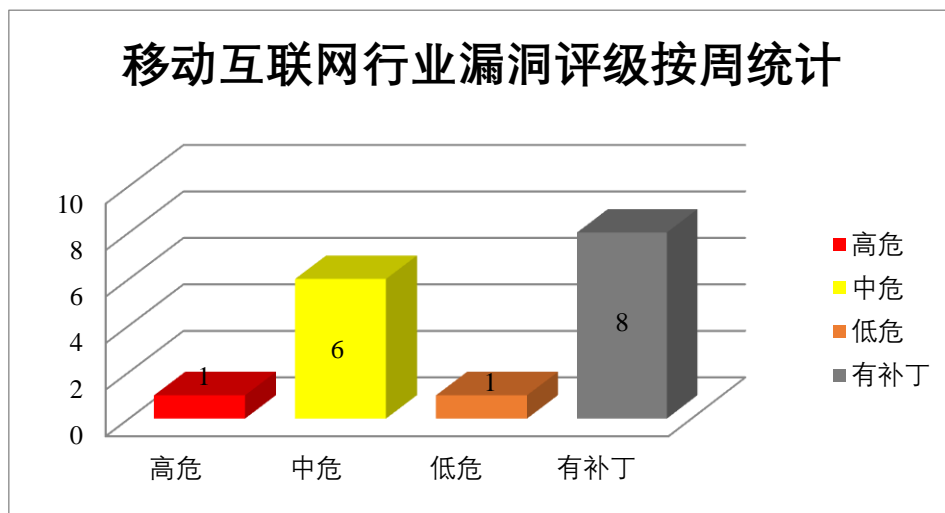


图 4 移动互联网行业漏洞统计

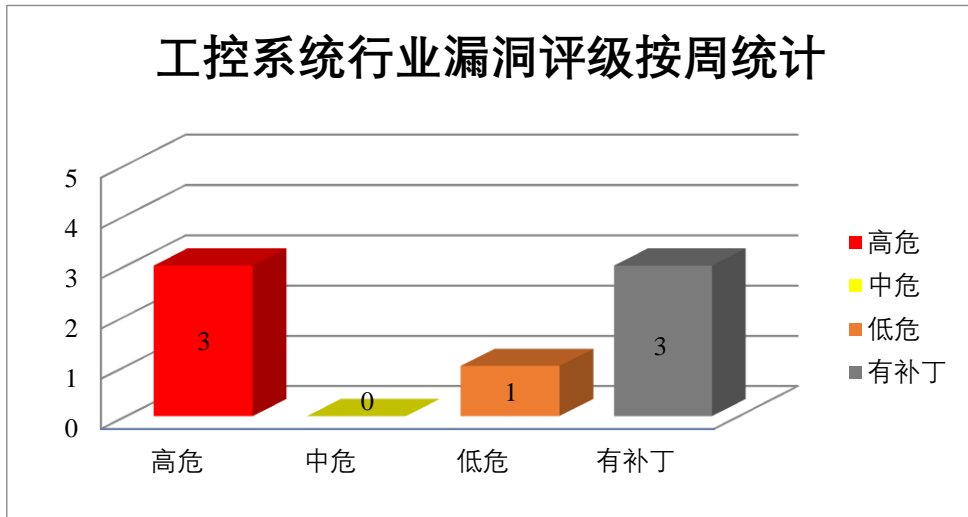


图 5 工控系统行业漏洞统计

## 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、Adobe 产品安全漏洞

Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。Adobe Connect 是美国奥多比（Adobe）公司的一个用于创建会议环境的软件。Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。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，导致敏感内存泄露等。

CNVD 收录的相关漏洞包括：Adobe Animate 整数溢出或环绕漏洞、Adobe Animate 越界写入漏洞（CNVD-2024-48896）、Adobe Animate 内存错误引用漏洞（CNVD-2024-48905）、Adobe Connect 跨站脚本漏洞（CNVD-2024-48907、CNVD-2024-48908）、Adobe InDesign 堆栈缓冲区溢出漏洞、Adobe InDesign 越界读取漏洞（CNVD-2024-48911、CNVD-2024-48912）。其中，“Adobe Animate 整数溢出或环绕漏洞、Adobe Animate 越界写入漏洞（CNVD-2024-48896）、Adobe Animate 内存错误引用漏洞（CNVD-2024-48905）、Adobe InDesign 堆栈缓冲区溢出漏洞”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-2024-48897>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-48896>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-48905>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-48907>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-48909>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-48908>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-48911>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-48912>

## 2、Apache 产品安全漏洞

Apache Hive 是美国阿帕奇 (Apache) 基金会的一套基于 Hadoop (分布式系统基础架构) 的数据仓库软件。该软件提供了一个数据集成方法和一种高级的查询语言, 以支持在 Hadoop 上进行大规模数据分析。Apache Tomcat 是美国阿帕奇 (Apache) 基金会的一款轻量级 Web 应用服务器。用于实现对 Servlet 和 JavaServer Page (JSP) 的支持。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 Kafka 是美国阿帕奇 (Apache) 基金会的一套开源的分布式流媒体平台。该平台能够获取实时数据, 用于构建对数据流的变化进行实时反应的应用程序。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 Solr 是美国阿帕奇 (Apache) 基金会的一款基于 Lucene (一款全文搜索引擎) 的搜索服务器。该产品支持层面搜索、垂直搜索、高亮显示搜索结果等。Apache ZooKeeper 是 Apache 软件基金会下一项集中式服务, 用于维护配置信息、命名、提供分布式同步以及提供组服务。Apache Traffic Server 是一个高性能的缓存代理服务器, 用于加速 Web 应用和内容分发网络。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 ConfigProviders 读取磁盘和环境变量中的任意内容, 提升权限, 导致远程代码执行等。

CNVD 收录的相关漏洞包括: Apache Hive 代码执行漏洞、Apache Tomcat 资源管理问题漏洞 (CNVD-2024-49151)、Apache CloudStack 输入验证错误漏洞 (CNVD-2024-49156)、Apache Kafka 授权问题漏洞、Apache Arrow 反序列化漏洞 (CNVD-2024-49154)、Apache Solr 代码问题漏洞、Apache ZooKeeper 身份验证绕过漏洞、Apache Traffic Server 权限提升漏洞 (CNVD-2024-49157)。其中, 除“Apache Tomcat 资源管理问题漏洞 (CNVD-2024-49151)、Apache Kafka 授权问题漏洞”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-2024-49152>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49151>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49156>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49155>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49154>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49159>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49158>

<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49157>

### 3、IBM 产品安全漏洞

IBM Db2 是美国国际商业机器（IBM）公司的一套关系型数据库管理系统。该系统的执行环境主要有 UNIX、Linux、IBMi、z/OS 以及 Windows 服务器版本。IBM Carbon Design System 是一套用于构建用户界面的设计系统。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。IBM Data Virtualization Manager 是美国国际商业机器（IBM）公司的一个通用查询引擎，可跨数据库、数据仓库、数据湖和流数据执行分布式和虚拟化查询。IBM Cognos Controller 是美国国际商业机器（IBM）公司的一套商业智能与计划解决方案。该产品具有流程自动化、财务审计控制、创建和管理财务报告等功能。IBM AIX 是美国国际商业机器（IBM）公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM Security Verify AccessAppliance 是基于网络设备的安全解决方案，提供基于 Web 的威胁的访问控制和保护。IBM Jazz Foundation 是美国国际商业机器（IBM）公司的一个面向软件交付技术的下一代协作平台。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命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Db2 拒绝服务漏洞（CNVD-2024-49168）、IBM Carbon Design System 跨站脚本漏洞、IBM InfoSphere Information Server 输入验证错误漏洞（CNVD-2024-49166）、IBM Data Virtualization Manager 代码执行漏洞、IBM Cognos Controller 文件上传漏洞（CNVD-2024-49171）、IBM AIX 操作系统命令注入漏洞、IBM Security Verify Access Appliance 硬编码漏洞、IBM Jazz Foundation 跨站脚本漏洞（CNVD-2024-49173）。其中，“IBM Data Virtualization Manager 代码执行漏洞、IBM Cognos Controller 文件上传漏洞（CNVD-2024-49171）、IBM Security Verify Access Appliance 硬编码漏洞”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-2024-49168>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49167>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49166>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49172>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49171>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49169>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49174>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49173>

### 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。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，攻击者可利用漏洞绕过安全限制，提升权限，获取敏感信息。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2024-49501、CNVD-2024-49505、CNVD-2024-49506、CNVD-2024-49507、CNVD-2024-49508）、Google Android 权限提升漏洞（CNVD-2024-49502、CNVD-2024-49503）、Google Chrome 安全绕过漏洞（CNVD-2024-49509）。其中，“Google Android 权限提升漏洞（CNVD-2024-49502）、Google Chrome 安全绕过漏洞（CNVD-2024-49509）”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-2024-49501>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49502>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49503>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49505>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49506>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49507>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49508>  
<https://www.cnvd.org.cn/flaw/show/CNVD-2024-49509>

## 5、D-Link DAP-1513 拒绝服务漏洞

D-Link DAP-1513 是中国友讯（D-Link）公司的一款无线网桥。本周，D-Link DAP-1513 被披露存在拒绝服务漏洞，攻击者可利用该漏洞导致拒绝服务。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-2024-49512>

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-2024-49215	Microsoft Defender 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49057">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49057</a>
CNVD-2024-48895	Adobe Animate 访问未初始化指针漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://helpx.adobe.com/security/products/animate/apsb24-96.html">https://helpx.adobe.com/security/products/animate/apsb24-96.html</a>
CNVD-2024-49516	Delta Electronics DRASimuCAD ICS 解析越界写代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： <a href="https://www.deltaww.com/">https://www.deltaww.com/</a>
CNVD-2024	Adobe Animate 空指针解引	高	厂商已发布了漏洞修复程序，请及

-48894	用漏洞 (CNVD-2024-48894)		时关注更新： <a href="https://helpx.adobe.com/security/products/animate/apsb24-96.html">https://helpx.adobe.com/security/products/animate/apsb24-96.html</a>
CNVD-2024-49205	Craft CMS 未经身份验证远程代码执行漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新： <a href="https://craftcms.com">https://craftcms.com</a>
CNVD-2024-49216	Microsoft Excel 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49069">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49069</a>
CNVD-2024-49514	Rockwell Automation Power Monitor 1000 设备接管漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1714.html">https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1714.html</a>
CNVD-2024-49515	Delta Electronics DRASimuCAD STP 解析类型混淆代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： <a href="https://www.deltaww.com/">https://www.deltaww.com/</a>
CNVD-2024-48898	Adobe Animate 输入验证不正确漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://helpx.adobe.com/security/products/animate/apsb24-96.html">https://helpx.adobe.com/security/products/animate/apsb24-96.html</a>
CNVD-2024-49212	Microsoft Update Catalog 反序列化漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49147">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49147</a>

小结：本周，Adobe 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，导致敏感内存泄露等。此外，Apache、IBM、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，提升权限，获取敏感信息，在系统上执行任意命令，导致拒绝服务等。另外，D-Link DAP-1513 被披露存在拒绝服务漏洞，攻击者可利用该漏洞导致拒绝服务。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、TOTOLINK AC1200 setWizardCfg 函数缓冲区溢出漏洞

#### 验证描述

TOTOLINK AC1200 是中国吉翁电子(TOTOLINK)公司的一款双频 Wi-Fi 路由器。TOTOLINK AC1200 v4.1.5cu.861\_B20230220 版本存在缓冲区溢出漏洞，该漏洞源



于在 setWizardCfg 函数的 ssid5g 参数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/TTTJJJWW/AHU-IoT-vulnerable/blob/main/TOTOLINK/AC1200T8/setWizardCfg.md>

参考链接: <https://www.cnvd.org.cn/flaw/show/CNVD-2024-49499>

### 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. Palo Alto 防火墙存在安全漏洞，触发无需交互和权限

Palo Alto Networks 近日披露，其下一代防火墙中的 PAN-OS 软件存在一个安全漏洞，编号为 CVE-2024-3393。该漏洞允许未经身份验证的攻击者通过发送精心构造的 DNS 数据包，利用 DNS 安全特性触发拒绝服务（DoS）状态。若此漏洞被反复利用，可能导致受影响的防火墙重启并进入维护模式。

参考链接: <https://www.freebuf.com/news/418628.html>

### 2. Apache HugeGraph-Server 漏洞让攻击者绕过身份验证

Apache HugeGraph-Server（一种广泛使用的开源图形数据库系统）中发现了一个新的安全漏洞 CVE-2024-43441，是由于服务器内未正确处理身份验证机制而引起。

参考链接: <https://cybersecuritynews.com/apache-hugegraph-server-vulnerability/>

## 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](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82991537