国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 12 月 09 日-2024 年 12 月 15 日　　2024 年第 50 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 295 个，其中高危漏洞 158 个、中危漏洞 115 个、低危漏洞 22 个。漏洞平均分值为 6.51。本周收录的漏洞中，涉及 0day 漏洞 224 个（占 76%），其中互联网上出现“Tenda AC 10 formSetDeviceName 函数堆栈溢出漏洞、FreePBX 文件上传漏洞”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 38375 个，与上周（8839 个）环比增加 334%。

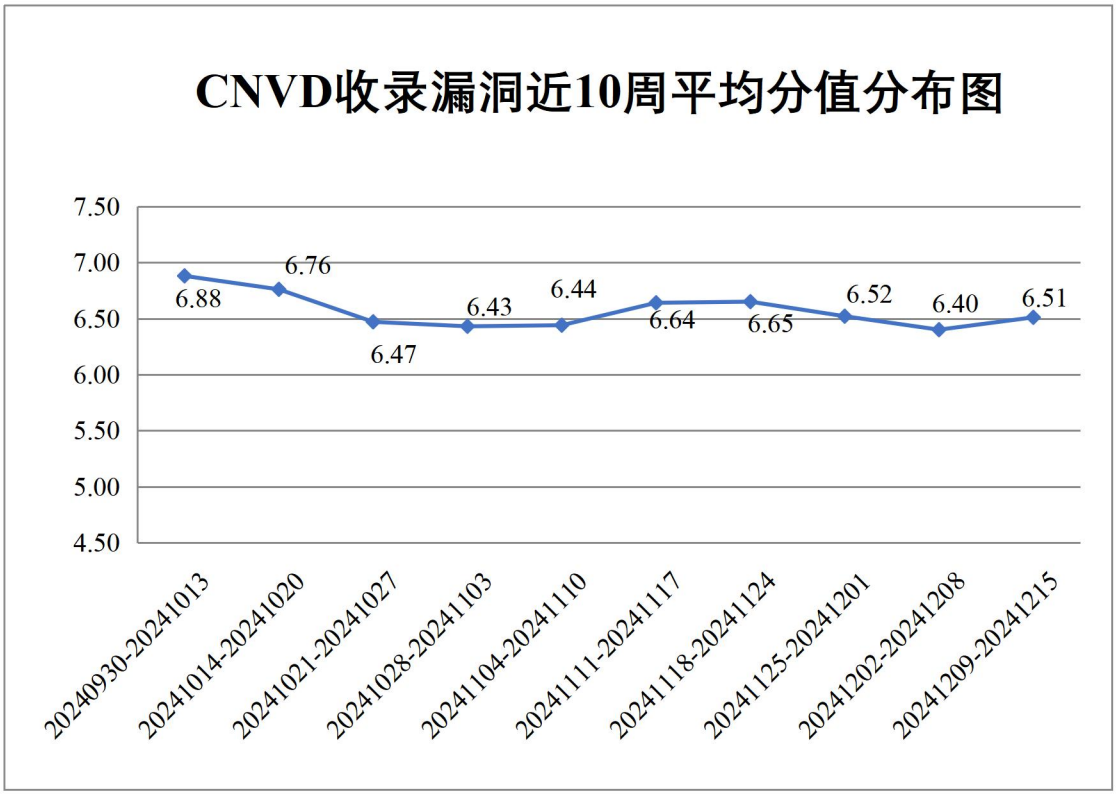

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 5 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 893 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 107 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 10 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：

卓智网络科技有限公司、重庆中联信息产业有限责任公司、重庆梅安森科技股份有限公司、中新网络信息安全股份有限公司、中文在线集团股份有限公司、中科方德软件有限公司、中建材信云智联科技有限公司、智慧互通科技股份有限公司、智互联（深圳）科技有限公司、智恒科技股份有限公司、浙江蓝鸽科技有限公司、浙江兰德纵横网络技术股份有限公司、友讯电子设备（上海）有限公司、优视科技有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、小米科技有限责任公司、夏普商贸（中国）有限公司、武汉天地伟业科技有限公司、唯智信息技术（上海）股份有限公司、统信软件技术有限公司、同望科技股份有限公司、天地伟业技术有限公司、腾讯安全应急响应中心、苏州真趣信息科技有限公司、四创科技有限公司、四川迅睿云软件开发有限公司、深圳崖山科技有限公司、深圳维盟科技股份有限公司、深圳市月歌科技有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市安之源电子有限公司、申瓯通信设备有限公司、上海真兰仪表科技股份有限公司、上海万户信息技术有限公司、上海茸易科技有限公司、上海繁易信息科技股份有限公司、上海博达数据通信有限公司、上海宝信软件股份有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山东思达特测控设备有限公司、厦门天锐科技股份有限公司、厦门四信物联网科技有限公司、任子行网络技术股份有限公司、青岛海信网络科技股份有限公司、青岛高校信息产业股份有限公司、麒麟软件有限公司、普联技术有限公司、品茗科技股份有限公司、鹏为软件股份有限公司、南京南软科技有限公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、领航未来（北京）科技有限公司、乐众信息技术股份有限公司、朗坤智慧科技股份有限公司、柯尼卡美能达集团、矩阵起源（深圳）信息科技有限公司、江苏传智播客教育科技股份有限公司、佳瑛科技有限公司、吉翁电子（深圳）有限公司、湖南众合百易信息技术有限公司、湖南省众达数蔚信息技术有限公司、黑龙江省创新农业物权融资有限公司、河北品科信息科技有限公司、杭州雄伟科技开发股份有限公司、杭州微宏科技有限公司、杭州三汇信息工程有限公司、杭州海康威视数字技术股份有限公司、杭州安恒信息技术股份有限公司、广州市动景计算机科技有限公司、广州赛意信息科技股份有限公司、广州红帆科技有限公司、广东数夫软件有限公司、广东国星科技有限公司、广东保伦电子股份有限公司、烽火通信科技股份有限公司、东莞市同享软件科技有限公司、丹东新北方通讯电器有限公司、成都索贝数码科技股份有限公司、畅捷通

信息技术股份有限公司、北京中农信达信息技术有限公司、北京云帆互联科技有限公司、北京优锘科技有限公司、北京映翰通网络技术股份有限公司、北京星网锐捷网络技术有限公司、北京伟联科技有限公司、北京网御星云信息技术有限公司、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、北京时空智友科技有限公司、北京神州数码云计算有限公司、北京神州视翰科技有限公司、北京龙软科技股份有限公司、北京金和网络股份有限公司、北京和欣运达科技有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、奥琦玮信息科技（北京）有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安徽新中新华科电子股份有限公司和安徽皖通邮电股份有限公司。

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、新华三技术有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。中孚安全技术有限公司、北京时代新威信息技术有限公司、北京翰慧投资咨询有限公司、北京纽盾网安信息技术有限公司、北京天下信安技术有限公司、河南东方云盾信息技术有限公司、联通数字科技有限公司、北京航空航天大学、苏州棱镜七彩信息科技有限公司、北京众安天下科技有限公司、平安银河实验室、北京网御星云信息技术有限公司、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、淮安易云科技有限公司、贵州多彩网安科技有限公司、杭州默安科技有限公司、成都安美勤信息技术股份有限公司、上海观安信息技术股份有限公司、北京安帝科技有限公司、福建福诺移动通信技术有限公司、北京远禾科技有限公司、上海蜚语信息科技有限公司、北京山石网科信息技术有限公司、信息产业信息安全测评中心、北京君云天下科技有限公司、成都久信信息技术股份有限公司、中资网络信息安全科技有限公司、深圳昂楷科技有限公司、中华人民共和国广东海事局、上海吨吨信息技术有限公司、宁夏凯信特信息科技有限公司、江苏百达智慧网络科技有限公司（含光实验室）、上海维信荟智金融科技有限公司、四川汉安数智科技有限公司、国网浙江省电力有限公司电力科学研究院、广西玉柴机器集团有限公司及其他个人白帽子向 CNVD 提交了 38375 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 36996 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）	20266	20266
奇安信网神（补天平	15161	15161

台）		
三六零数字安全科技集团有限公司	1196	1196
北京启明星辰信息安全技术有限公司	1109	14
新华三技术有限公司	1061	0
北京天融信网络安全技术有限公司	504	72
北京神州绿盟科技有限公司	406	1
深信服科技股份有限公司	395	1
上海交大	373	373
阿里云计算有限公司	335	5
北京数字观星科技有限公司	276	0
安天科技集团股份有限公司	270	0
杭州安恒信息技术股份有限公司	206	64
中国电信集团系统集成有限责任公司	92	0
北京知道创宇信息技术有限公司	52	0
远江盛邦（北京）网络安全科技股份有限公司	35	35
京东科技信息技术有限公司	26	26
北京升鑫网络科技有限公司（青藤云安全）	21	21
北京长亭科技有限公司	19	3
南京众智维信息科技有限公司	15	15

杭州迪普科技股份有限公司	15	0
北京安信天行科技有限公司	9	9
中孚安全技术有限公司	23	23
北京时代新威信息技术有限公司	16	16
北京翰慧投资咨询有限公司	13	13
西门子（中国）有限公司	10	0
北京纽盾网安信息技术有限公司	9	9
北京天下信安技术有限公司	9	9
河南东方云盾信息技术有限公司	8	8
联通数字科技有限公司	7	7
北京航空航天大学	6	6
苏州棱镜七彩信息科技有限公司	6	6
北京众安天下科技有限公司	5	5
平安银河实验室	5	5
北京网御星云信息技术有限公司	5	5
成都卫士通信息安全技术有限公司	4	4
江苏云天网络安全技术有限公司	4	4
淮安易云科技有限公司	4	4
贵州多彩网安科技有	3	3

限公司		
杭州默安科技有限公司	3	3
成都安美勤信息技术股份有限公司	2	2
上海观安信息技术股份有限公司	2	2
北京安帝科技有限公司	2	2
福建福诺移动通信技术有限公司	2	2
北京远禾科技有限公司	2	2
上海蜚语信息科技有限公司	2	2
北京山石网科信息技术有限公司	2	2
信息产业信息安全测评中心	2	2
北京君云天下科技有限公司	1	1
成都久信信息技术股份有限公司	1	1
中资网络信息安全科技有限公司	1	1
深圳昂楷科技有限公司	1	1
中华人民共和国广东海事局	1	1
上海吨吨信息技术有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
江苏百达智慧网络科技有限公司（含光实	1	1

验室）		
上海维信荟智金融科技有限公司	1	1
四川汉安数智科技有限公司	1	1
国网浙江省电力有限公司电力科学研究院	1	1
广西玉柴机器集团有限公司	1	1
CNCERT 宁夏分中心	5	5
个人	950	950
报送总计	42965	38375

本周漏洞按类型和厂商统计

本周，CNVD 收录了 295 个漏洞。WEB 应用 137 个，网络设备（交换机、路由器等网络端设备）61 个，应用程序 60 个，操作系统 20 个，智能设备（物联网终端设备）14 个，安全产品 2 个，数据库 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	137
网络设备（交换机、路由器等网络端设备）	61
应用程序	60
操作系统	20
智能设备（物联网终端设备）	14
安全产品	2
数据库	1

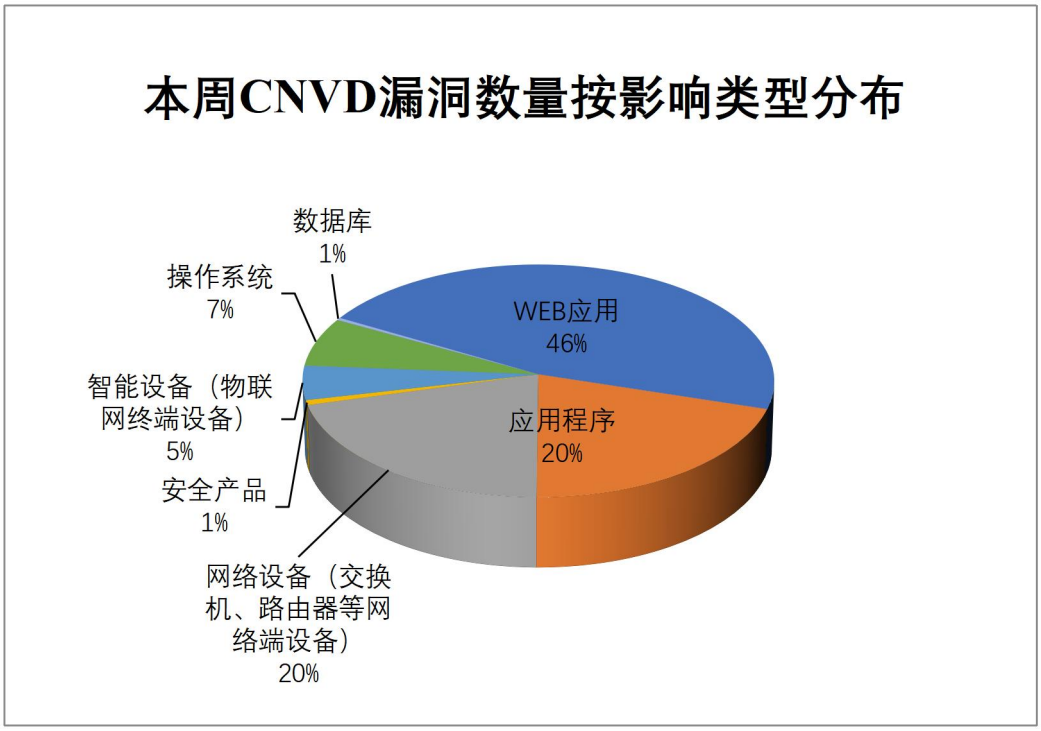

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、北京金和网络股份有限公司、畅捷通信息技术股份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	Google	13	5%
2	北京金和网络股份有限公司	11	4%
3	畅捷通信息技术股份有限公司	11	4%
4	Siemens	10	3%
5	Apache	10	3%
6	Adobe	10	3%
7	IBM	9	3%
8	深圳市蓝凌软件股份有限公司	8	3%
9	深圳市吉祥腾达科技有限公司	7	2%
10	其他	206	70%

本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞，11 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，“Google Android 权限提升漏洞（CNVD-2024-47698）、Siemens RUGGEDCOM ROX II 跨站请求伪造漏洞”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/

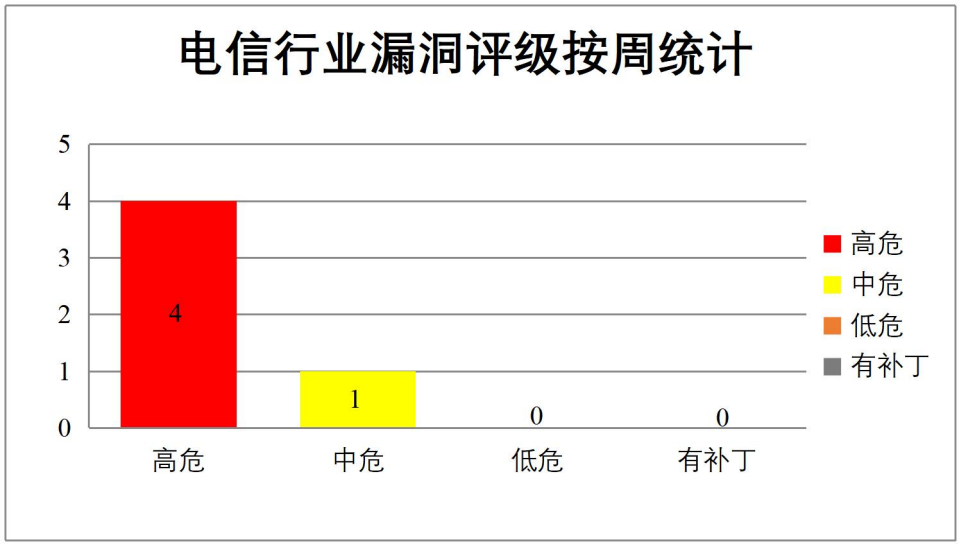

图 3 电信行业漏洞统计

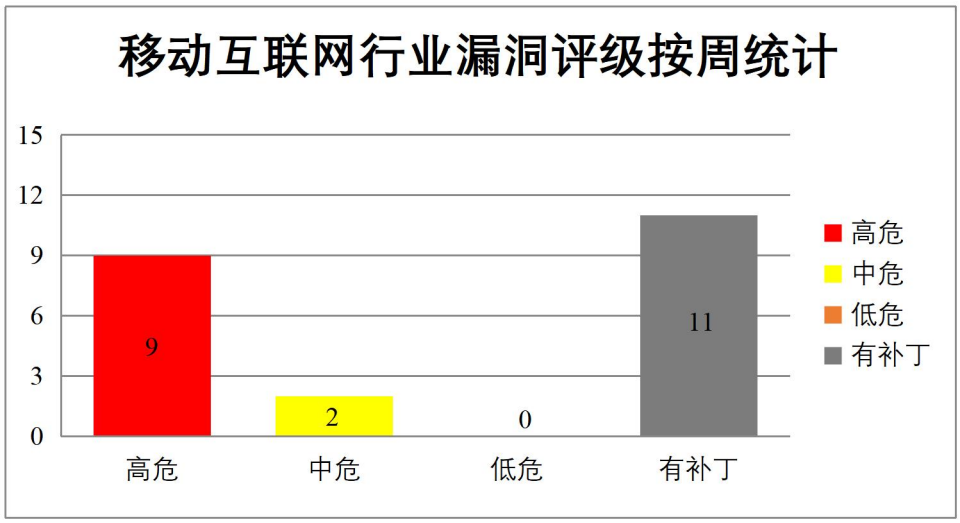

图 4 移动互联网行业漏洞统计

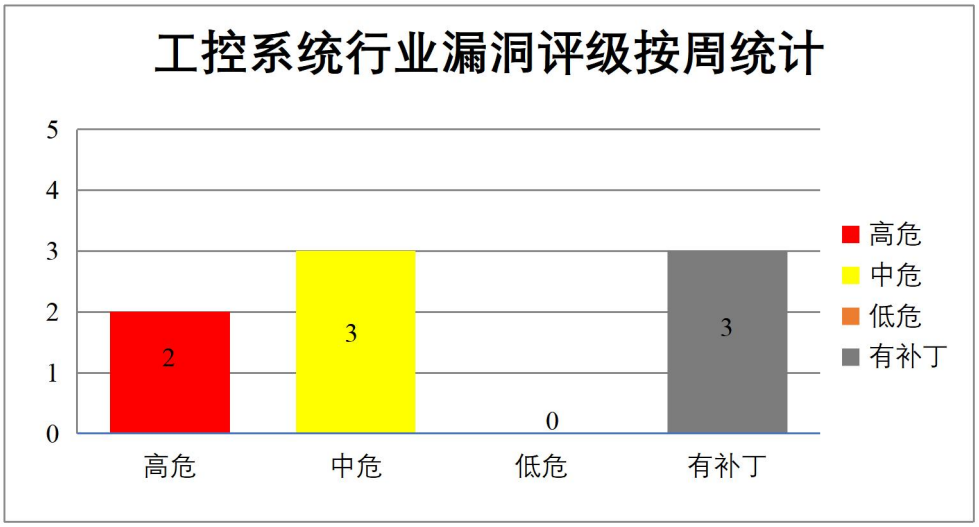

图 5 工控系统行业漏洞统计

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 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 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，攻击者可利用漏洞导致敏感内存泄露，在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Illustrator 越界读取漏洞（CNVD-2024-47504）、Adobe InDesign 堆缓冲区溢出漏洞（CNVD-2024-47505、CNVD-2024-47506）、Adobe InDesign 越界读取漏洞（CNVD-2024-47507、CNVD-2024-47508）、Adobe Illustrator 越界写入漏洞（CNVD-2024-47510、CNVD-2024-47513）、Adobe Illustrator 堆缓冲区溢出漏洞（CNVD-2024-47509）。其中，除“Adobe Illustrator 越界读取漏洞（CNVD-2024-47504）、Adobe InDesign 越界读取漏洞（CNVD-2024-47507、CNVD-2024-47508）”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-2024-47504
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47505
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47506
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47507
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47508
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47510
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47509

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47513

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，攻击者可利用漏洞提升权限，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2024-47698、CNVD-2024-47700、CNVD-2024-47699、CNVD-2024-47701、CNVD-2024-47702、CNVD-2024-47705、CNVD-2024-47707）、Google Android 代码执行漏洞（CNVD-2024-47706）。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-2024-47698

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47700

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47699

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47701

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47702

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47705

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47707

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47706

3、IBM 产品安全漏洞

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 App Connect Enterprise 是 IBM 公司的一个操作系统。IBM App Connect Enterprise 将现有业界信任的 IBM Integration Bus 技术与 IBM App Connect Professional 以及新的云本机技术进行了组合，提供一个可满足现代数字企业全面集成需求的平台。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。IBM Cloud Pak for Data 是美国国际商业机器（IBM）公司的一种云原生解决方案，可以让客户快速高效地使用数据和分析数据。IBM Maximo Application Suite 是美国国际商业机器（IBM）公司的一个为智能资产管理、监控、维护、计算机视觉。安全性和可靠性提供的单一平台。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。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，在系统上执行任意命令，导致意外状态，甚至导致崩溃等。

CNVD 收录的相关漏洞包括：IBM Cognos Controller 加密问题漏洞（CNVD-2024-47515）、IBM App Connect Enterprise 操作系统命令注入漏洞、IBM Jazz Foundation 访问控制错误漏洞、IBM Cloud Pak for Data 资源管理错误漏洞、IBM Cognos Contro

ller 信任管理问题漏洞（CNVD-2024-47517）、IBM Cognos Controller 跨站请求伪造漏洞、IBM Maximo Application Suite 跨站脚本漏洞、IBM Security Verify Access Appliance 操作系统命令注入漏洞。其中，除 “IBM Cognos Controller 加密问题漏洞（CNVD-2024-47515）、IBM Jazz Foundation 访问控制错误漏洞、IBM Maximo Application Suite 跨站脚本漏洞”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-2024-47515
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47514
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47519
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47518
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47517
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47516
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47522
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47520

4、Apache 产品安全漏洞

Apache NimBLE 是美国阿帕奇（Apache）基金会的一个开源蓝牙 5.4 堆栈（主机和控制器），完全取代 Nordic 芯片组上的专有 SoftDevice。它是 Apache Mynewt 项目的一部分。Apache Ozone 是美国阿帕奇（Apache）基金会的一个应用软件。一个面向 Hadoop 和云原生环境的可伸缩，冗余和分布式对象存储。Apache HertzBeat 是美国阿帕奇（Apache）公司的一个可以监控各种组件的工具。Apache Roller 是美国阿帕奇（Apache）基金会的一套基于 Java 的多用户开源博客系统。Apache Struts 是美国阿帕奇（Apache）基金会的一个开源项目，是一套用于创建企业级 Java Web 应用的开源 MVC 框架，主要提供两个版本框架产品，Struts 1 和 Struts 2。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的令牌信息，提升权限，上传恶意文件，在系统上执行任意命令等。

CNVD 收录的相关漏洞包括：Apache NimBLE 缓冲区溢出漏洞、Apache NimBLE 越界读取漏洞、Apache Ozone 身份验证错误漏洞、Apache HertzBeat 反序列化漏洞（CNVD-2024-47713）、Apache HertzBeat 信息泄露漏洞、Apache HertzBeat 命令注入漏洞、Apache Roller 跨站请求伪造漏洞（CNVD-2024-47716）、Apache Struts 文件上传漏洞。其中，除“Apache NimBLE 缓冲区溢出漏洞、Apache Roller 跨站请求伪造漏洞（CNVD-2024-47716）”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-2024-47711
https://www.cnvd.org.cn/flaw/show/CNVD-2024-47710

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47709

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47713

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47715

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47714

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47716

https://www.cnvd.org.cn/flaw/show/CNVD-2024-47916

5、Tenda i9 拒绝服务漏洞

Tenda i9 是中国腾达（Tenda）公司的一种可以在天花板上安装的无线接入点。本周，Tenda i9 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-2024-48103

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-2024-47906	Siemens Parasolid 越界写入漏洞（CNVD-2024-47906）	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://cert-portal.siemens.com/productcert/html/ssa-979056.html
CNVD-2024-47518	IBM Cloud Pak for Data 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：https://www.ibm.com/support/pages/node/7177065
CNVD-2024-47699	Google Android 权限提升漏洞（CNVD-2024-47699）	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/2024-11-01
CNVD-2024-47701	Google Android 权限提升漏洞（CNVD-2024-47701）	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/2024-11-01
CNVD-2024-47708	WordPress 插件 WP Umbrella: Update Backup Restore & Monitoring 本地文件包含漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-health/wp-umbrella-update-backup-restore-monitoring-2170-unauthenticated-local-file-inclusion
CNVD-2024	Apache HertzBeat 命令注入	高	厂商已发布了漏洞修复程序，请及

-47714	漏洞		时关注更新：https://lists.apache.org/thread/gvbc68krhqhht7mkkkx7k13k6k6fdhy0
CNVD-2024-47910	Siemens Solid Edge V2024 堆缓冲区溢出漏洞	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://cert-portal.siemens.com/productcert/html/ssa-730188.html
CNVD-2024-47909	Siemens Solid Edge V2024 堆缓冲区溢出漏洞（CNVD-2024-47909）	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://cert-portal.siemens.com/productcert/html/ssa-730188.html
CNVD-2024-47517	IBM Cognos Controller 信任管理问题漏洞（CNVD-2024-47517）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7177220
CNVD-2024-47908	Siemens Solid Edge V2024 整数下溢漏洞	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://cert-portal.siemens.com/productcert/html/ssa-730188.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞导致敏感内存泄露，在当前用户的上下文中执行任意代码。此外，Google、IBM、Apache 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，上传恶意文件，在系统上执行任意命令等。另外，Tenda i9 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、Tenda AC10 formSetDeviceName 函数堆栈溢出漏洞

验证描述

Tenda AC10 是一款无线路由器。

Tenda AC10 formSetDeviceName 函数存在堆栈溢出漏洞，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导致拒绝服务。

验证信息

POC 链接：https://github.com/z1r00/IOT_Vul/blob/main/Tenda/AC10/formSetDeviceName/readme.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-48102

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. 大众和斯柯达曝 12 个组合漏洞，攻击者可在 10 米内无接触入侵

网络安全研究人员发现斯柯达和大众汽车的某些车型的车载娱乐系统中存在多个漏洞，这些漏洞可能让黑客远程跟踪并访问用户的敏感数据。

参考链接：https://cybersecuritynews.com/vulnerabilities-skoda-volkswagen-cars/

2. 关键的 Windows UI 自动化框架漏洞允许黑客绕过 EDR

攻击者利用了 Windows UIA 来执行多种恶意活动，可巧妙地避开端点检测和响应（EDR）解决方案的监控。

参考链接：https://thehackernews.com/2024/12/new-malware-technique-could-exploit.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