国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 10 月 28 日-2024 年 11 月 03 日 **2024 年第 44 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 237 个，其中高危漏洞 113 个、中危漏洞 107 个、低危漏洞 17 个。漏洞平均分值为 6.43。本周收录的漏洞中，涉及 0day 漏洞 158 个（占 67%），其中互联网上出现“TOTOLINK X5000R 和 A7000R 缓冲区溢出漏洞（CNVD-2024-42443）、OneBlog Lab 模块跨站脚本漏洞”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 9485 个，与上周（5074 个）环比增加 87%。

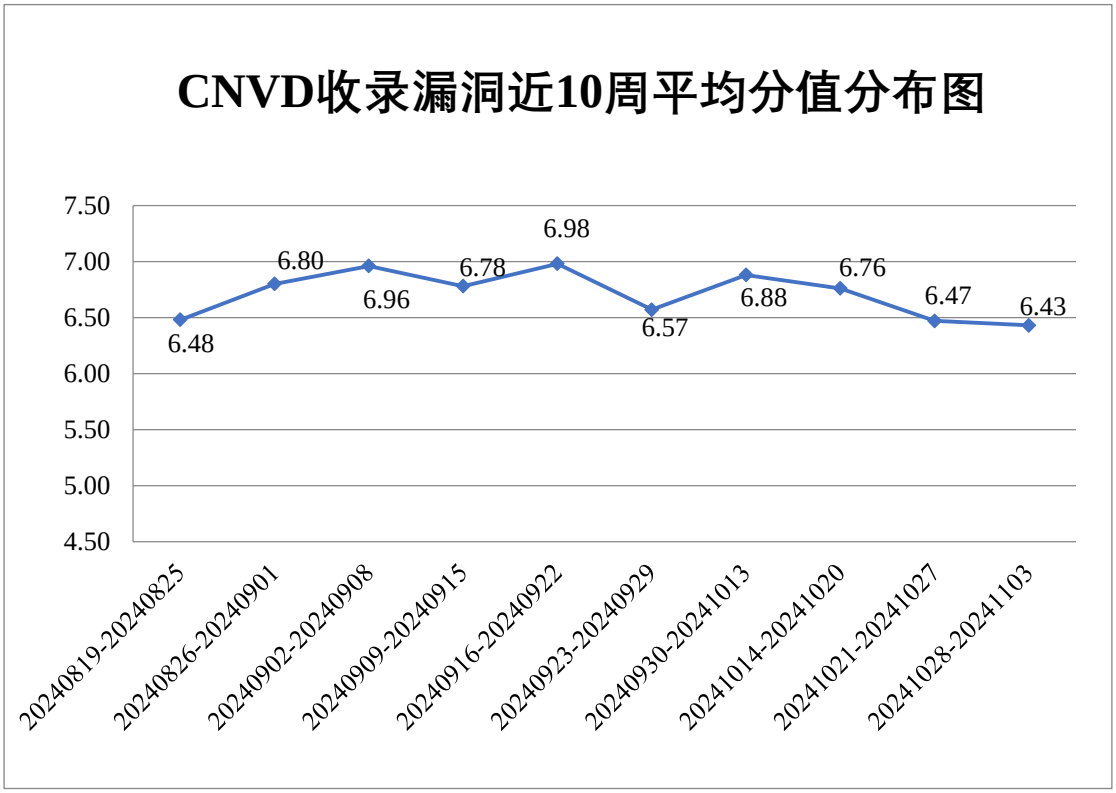

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 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 909 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 96 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 21 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：

渔翁信息技术股份有限公司、用友网络科技股份有限公司、西门子（中国）有限公司、苏州汇川联合动力系统股份有限公司、松下电器（中国）有限公司、四川掌上时代科技有限公司、石家庄和嘉科技有限公司、神州数码控股有限公司、深圳拓安信物联股份有限公司、深圳市亿玛信诺科技有限公司、深圳市思迅软件股份有限公司、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、深圳市必联电子有限公司、上海肯特仪表股份有限公司、上海孚盟软件有限公司、上海百胜软件股份有限公司、上海艾泰科技有限公司、山东金钟科技集团股份有限公司、瑞斯康达科技发展股份有限公司、青岛大数华创科技有限公司、麒麟软件有限公司、普元信息技术股份有限公司、普联技术有限公司、南京亚派科技股份有限公司、迈普通信技术股份有限公司、联奕科技股份有限公司、力合科技（湖南）股份有限公司、蓝鸽集团有限公司、江苏浪潮信息咨询有限公司、华硕电脑（上海）有限公司、湖南众合百易信息技术有限公司、杭州海康威视数字技术股份有限公司、国泰新点软件股份有限公司、广州同鑫科技有限公司、广联达科技股份有限公司、富士胶片商业创新（中国）有限公司、懂微信息技术（上海）有限公司、畅捷通信息技术股份有限公司、北京优锘科技股份有限公司、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、北京神州视翰科技有限公司、北京朗新天霁软件技术有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京慧同科技有限公司和 ABB（中国）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，天津市国瑞数码安全系统股份有限公司、新华三技术有限公司、北京启明星辰信息安全技术有限公司、深信服科技股份有限公司、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。成都卫士通信息安全技术有限公司、河南东方云盾信息技术有限公司、北京翰慧投资咨询有限公司、淮安易云科技有限公司、快页信息技术有限公司、江苏金盾检测技术股份有限公司、御维网络安全技术有限公司、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、上海谋乐网络科技有限公司、卫士通（广州）信息安全技术有限公司、苏州棱镜七彩信息科技有限公司、平安银河实验室、江苏云天网络安全技术有限公司、北京纽盾网安信息

技术有限公司、北京航空航天大学、南方电网科学研究院有限责任公司、联通数字科技有限公司、上海观安信息技术股份有限公司、中资网络信息安全科技有限公司、上海亿保健康科技集团有限公司、北京卓识网安技术股份有限公司、北京天下信安技术有限公司、河南灵创电子科技有限公司、安徽希客安全技术服务有限公司、安徽天行网安信息安全技术有限公司、北京威努特技术有限公司、深圳昂楷科技有限公司、成都久信信息技术股份有限公司、吉林省吉林祥云信息技术有限公司、超聚变数字技术有限公司、上海戎磐网络科技有限公司、河南宝通信息安全测评有限公司、北京星网锐捷网络技术有限公司、国家计算机病毒应急处理中心、江苏正信信息安全测试有限公司、深圳市博通智能技术有限公司及其他个人白帽子向 CNVD 提交了 9485 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 7582 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）	6691	6691
天津市国瑞数码安全系统股份有限公司	1587	0
新华三技术有限公司	811	0
北京启明星辰信息安全技术有限公司	734	5
三六零数字安全科技集团有限公司	713	713
深信服科技股份有限公司	621	3
北京神州绿盟科技有限公司	527	108
京东科技信息技术有限公司	407	0
北京数字观星科技有限公司	351	0
上海交大	178	178
阿里云计算有限公司	164	0
北京知道创宇信息技术有限公司	142	4
恒安嘉新（北京）科技股份公司	88	0

南京众智维信息科技有限公司	69	0
杭州安恒信息技术股份有限公司	53	7
远江盛邦（北京）网络安全科技股份有限公司	52	52
安天科技集团股份有限公司	49	0
北京天融信网络安全技术有限公司	46	19
北京长亭科技有限公司	27	2
北京升鑫网络科技有限公司（青藤云）	27	27
中国电信股份有限公司网络安全产品运营中心	25	25
深圳市腾讯计算机系统有限公司（玄武实验室）	22	22
杭州迪普科技股份有限公司	12	2
华为技术有限公司	6	6
北京智游网安科技有限公司	4	4
北京安信天行科技有限公司	3	3
北京信联数安科技有限公司	2	2
浪潮电子信息产业股份有限公司	2	2
杭州海康威视数字技术股份有限公司	240	240
成都卫士通信息安全	151	151

技术有限公司		
河南东方云盾信息技术有限公司	70	70
北京翰慧投资咨询有限公司	36	36
淮安易云科技有限公司	28	28
快页信息技术有限公司	25	25
江苏金盾检测技术股份有限公司	21	21
御维网络安全技术有限公司	12	12
北京时代新威信息技术有限公司	12	12
北京山石网科信息技术有限公司	10	10
上海谋乐网络科技有限公司	10	10
卫士通（广州）信息安全技术有限公司	10	10
苏州棱镜七彩信息科技有限公司	9	9
平安银河实验室	8	8
江苏云天网络安全技术有限公司	6	6
北京纽盾网安信息技术有限公司	6	6
北京航空航天大学	4	4
南方电网科学研究院有限责任公司	4	4
联通数字科技有限公司	4	4
上海观安信息技术股份有限公司	4	4

中资网络信息安全科技有限公司	3	3
上海亿保健康科技集团有限公司	3	3
北京卓识网安技术股份有限公司	3	3
北京天下信安技术有限公司	3	3
河南灵创电子科技有限公司	3	3
安徽希客安全技术服务有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2
北京威努特技术有限公司	2	2
深圳昂楷科技有限公司	1	1
成都久信信息技术股份有限公司	1	1
吉林省吉林祥云信息技术有限公司	1	1
超聚变数字技术有限公司	1	1
上海戎磐网络科技有限公司	1	1
河南宝通信息安全测评有限公司	1	1
北京星网锐捷网络技术有限公司	1	1
国家计算机病毒应急处理中心	1	1
江苏正信信息安全测试有限公司	1	1
深圳市博通智能技术	1	1

有限公司		
个人	909	909
报送总计	15023	9485

本周漏洞按类型和厂商统计

本周，CNVD 收录了 237 个漏洞。WEB 应用 120 个，网络设备（交换机、路由器等网络端设备）49 个，应用程序 38 个，操作系统 13 个，数据库 9 个，安全产品 6 个，智能设备（物联网终端设备）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	120
网络设备（交换机、路由器等网络端设备）	49
应用程序	38
操作系统	13
数据库	9
安全产品	6
智能设备（物联网终端设备）	2

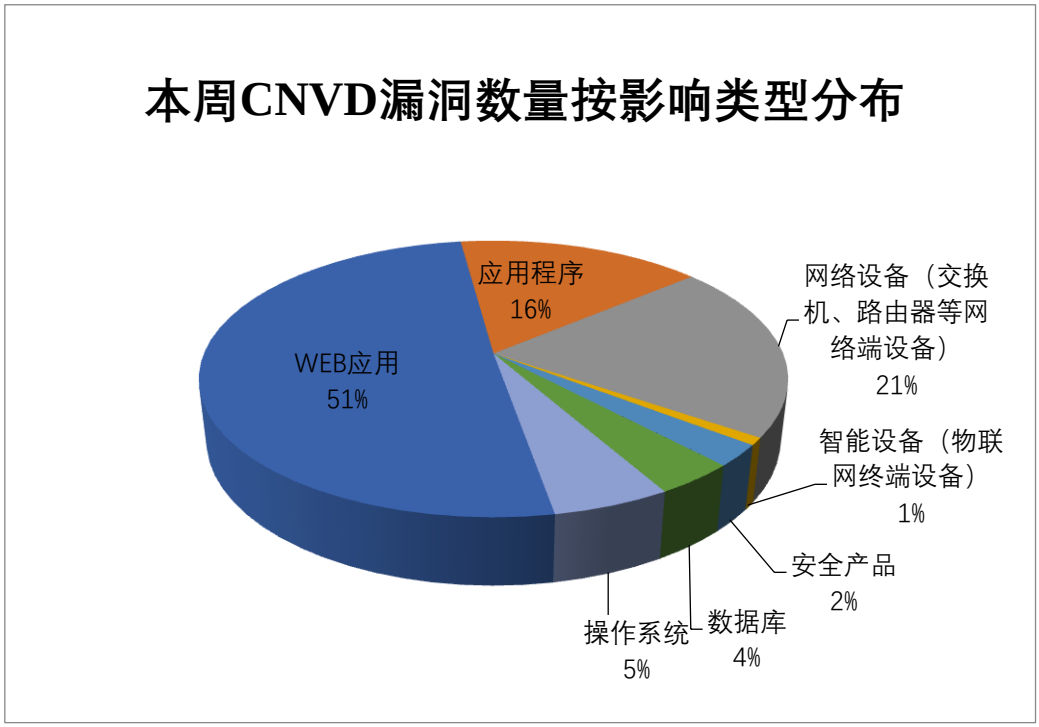

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用友网络科技股份有限公司、Microsoft、Google 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	用友网络科技股份有限公司	13	5%
2	Microsoft	13	5%
3	Google	11	5%
4	科华数据股份有限公司	10	4%
5	Moxa	10	4%
6	Adobe	9	4%
7	Oracle	9	4%
8	IBM	7	3%
9	Autodesk	6	3%
10	其他	149	63%

本周行业漏洞收录情况

本周，CNVD 收录了 34 个电信行业漏洞，10 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-2024-41856）、MOXA OnCell G3470A-LTE 命令注入漏洞”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/

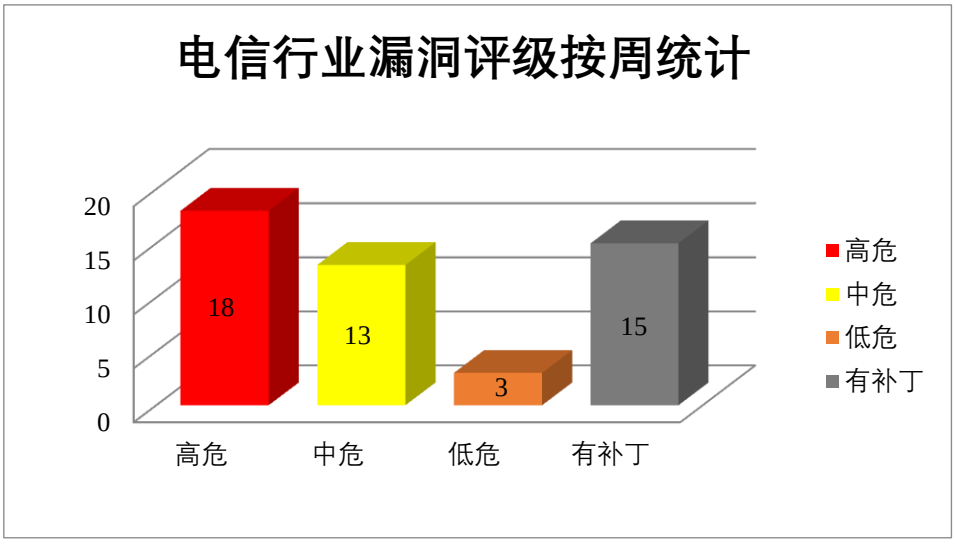

图 3 电信行业漏洞统计

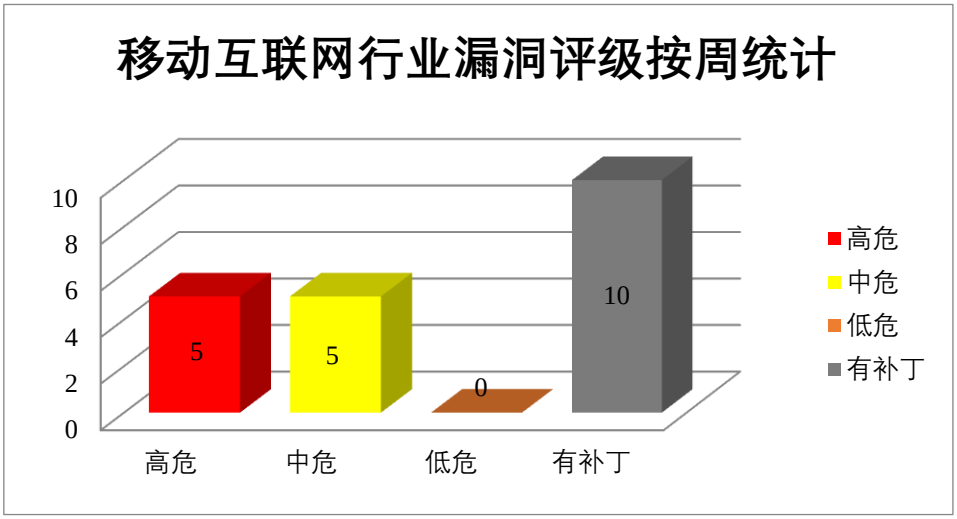

图 4 移动互联网行业漏洞统计

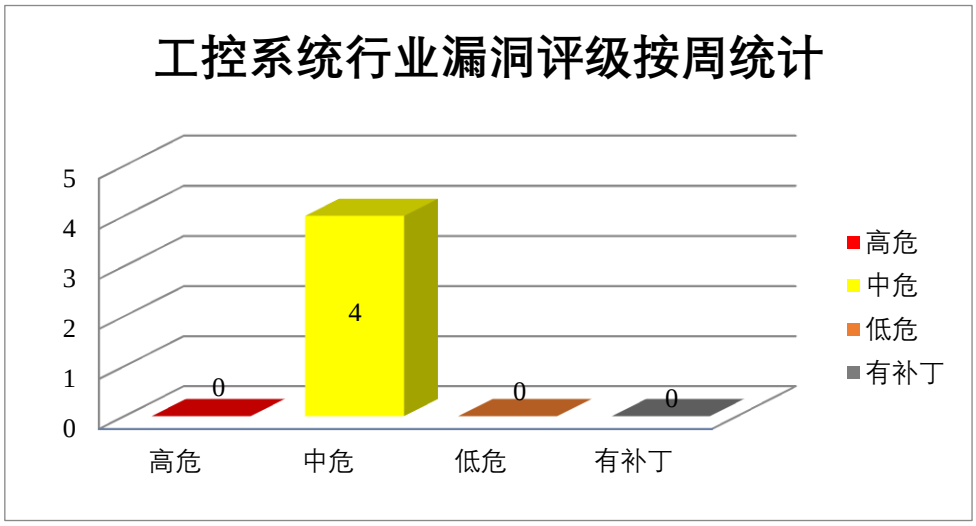

图 5 工控系统行业漏洞统计

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 Substance 3D Stager 是美国奥多比（Adobe）公司的一个虚拟 3D 工作室。Animate 是一款由 Adobe 开发的交互式矢量动画创作软件。Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。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，获取敏感信息，执行未经授权的操作，在当前用户环境中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Substance 3D Stager 缓冲区溢出漏洞（CNVD-2024-42107、CNVD-2024-42106、CNVD-2024-42109）、Adobe Substance 3D Stager

资源管理错误漏洞（CNVD-2024-42110）、Adobe Substance 3D Stager 代码执行漏洞（CNVD-2024-42108）、Adobe Animate 越界读取漏洞（CNVD-2024-42111）、Adobe Acrobat Reader 代码执行漏洞（CNVD-2024-42119）、Adobe Commerce 跨站请求伪造漏洞（CNVD-2024-42120）。其中，除“Adobe Animate 越界读取漏洞（CNVD-2024-42111）”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-2024-42107
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42106
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42110
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42109
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42108
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42111
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42119
https://www.cnvd.org.cn/flaw/show/CNVD-2024-42120

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。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，攻击者可利用漏洞获取敏感信息，升级权限，在系统上执行任意代码，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-2024-41855、CNVD-2024-41856、CNVD-2024-41861、CNVD-2024-41864）、Google Android NotificationManagerService.java 文件输入验证错误漏洞、Google Android 信息泄露漏洞（CNVD-2024-41862）、Google Android 拒绝服务漏洞（CNVD-2024-41863）、Google Chrome V8 代码执行漏洞（CNVD-2024-41865）。其中，除“Google Android 信息泄露漏洞（CNVD-2024-41862）、Google Android 拒绝服务漏洞（CNVD-2024-41863）”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-2024-41855
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41856
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41860
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41861
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41862
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41863
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41864
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41865

3、Microsoft 产品安全漏洞

Microsoft Edge 是美国微软（Microsoft）公司的一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft Office Visio 是美国微软（Microsoft）公司的 Office 软件系列中的负责绘制流程图和示意图的软件。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge (Chromium-based)远程代码执行漏洞（CNVD-2024-41984、CNVD-2024-41986、CNVD-2024-41987、CNVD-2024-41989、CNVD-2024-41990、CNVD-2024-41991）、Microsoft Office Visio 远程代码执行漏洞（CNVD-2024-41993、CNVD-2024-41994）。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-2024-41984
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41986
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41987
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41989
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41990
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41991
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41993
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41994

4、MOXA 产品安全漏洞

MOXA OnCell G3470A-LTE 是中国摩莎（MOXA）公司的系列蜂窝网关/路由器。MOXA Service 是中国摩莎（MOXA）公司的一个硬件设备基础服务。MOXA ioLogik E1200 Series 是中国摩莎（MOXA）公司的一系列通用控制器和 I/O 设备。MOXA EDS-4000/G4000 Series 是中国摩莎（MOXA）公司的一系列工业管理型以太网交换机。MOXA NPort W2150A/W2250A 是中国摩莎(MOXA)公司的一系列无线设备联网服务器。MOXA OnCell G3470A-LTE 是中国摩莎（MOXA）公司的系列蜂窝网关/路由器。MOXA ioLogik E1200 Series 是中国摩莎（MOXA）公司的一系列通用控制器和 I/O 设备。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，执行恶意操作，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：MOXA OnCell G3470A-LTE 命令注入漏洞（CNVD-2024-41848、CNVD-2024-41847）、MOXA Service 操作系统命令注入漏洞、MOXA ioLogik E1200 Series 跨站请求伪造漏洞、MOXA EDS-4000/G4000 Series 安全绕过漏洞、MOXA NPort W2150A/W2250A Series 缓冲区溢出漏洞、MOXA OnCell G3470A-LTE 缓冲区溢出漏洞、MOXA ioLogik E1200 Series 加密问题漏洞。其中，除“AMOXA EDS-4000/G4000 Series 安全绕过漏洞、MOXA ioLogik E1200 Series 加密问题漏洞”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-2024-41848
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41847
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41846
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41853
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41852
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41851
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41850
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41854

5、Tenda AX1806 sub_519F4 函数堆栈缓冲区溢出漏洞

Tenda AX1806 是中国腾达（Tenda）公司的一个 WiFi6 无线路由器。本周，Tenda AX1806 被披露存在堆栈缓冲区溢出漏洞，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。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-2024-42445

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-2024-41864	Google Android 权限提升漏洞（CNVD-2024-41864）	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/2024-05-01
CNVD-2024-41986	Microsoft Edge (Chromium-based)远程代码执行漏洞（CNVD-2024-41986）	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43587
CNVD-2024-41992	Microsoft Imagine Cup site 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38204
CNVD-2024-42105	Foxit Reader 资源管理错误漏洞（CNVD-2024-42105）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/support/security-bulletins.html
CNVD-2024-42113	IBM Aspera Console CSV 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://www.ibm.com/support/pages/node/7169765
CNVD-2024-42112	IBM ManageIQ 命令执行漏洞	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.manageiq.org/
CNVD-2024-42122	Foxit PDF Reader 释放后使用漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.foxit.com/support/security-bulletins.html
CNVD-2024-42347	Autodesk AutoCAD 内存错误引用漏洞（CNVD-2024-42347）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019
CNVD-2024-42349	Autodesk AutoCAD 堆溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019
CNVD-2024-42351	Autodesk AutoCAD 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019

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，获取敏感信息，执行未经授权的操作，在当前用户环境中执行任意代码。此外，Google、Microsoft、MOXA 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功能，获取敏感信息，执行未经授权的操作，执行任意代码，导致拒绝服务等。另外，Tenda AX1806 被披露存在堆栈缓冲区溢出漏洞，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。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 X5000R 和 A7000R 缓冲区溢出漏洞（CNVD-2024-42443）

验证描述

TOTOLINK X5000R 是一款路由器。TOTOLINK A7000R 是一款无线路由器。

TOTOLINK X5000R 和 A7000R 存在缓冲区溢出漏洞。攻击者可利用该漏洞通过命令字段造成拒绝服务（D0S）。

验证信息

POC 链接：https://github.com/ZIKH26/CVE-information/blob/master/TOTOLINK/Vul

nerability%20Information_2.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-42443

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. 开源 AI/ML 模型曝出 30 余个漏洞，可能导致远程代码执行与信息窃取风险

根据最新消息，开源人工智能（AI）和机器学习（ML）模型中已披露了三十几个安全漏洞，其中一些漏洞可能导致远程代码执行和信息窃取。

参考链接：https://www.freebuf.com/news/414008.html

2. 利用 Windows 漏洞，攻击者能降级系统组件恢复漏洞

据 Hackread 消息，在最近的一项研究中，SafeBreach Labs 研究员揭露了一种新的攻击技术，能够操纵 Windows 11 系统在更新时降级关键系统组件，从而让一些漏洞修复补丁失效。

参考链接：https://www.freebuf.com/news/413826.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