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 16 日-2024 年 12 月 22 日 **2024 年第 51 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 164 个，其中高危漏洞 106 个、中危漏洞 48 个、低危漏洞 10 个。漏洞平均分值为 6.89。本周收录的漏洞中，涉及 0day 漏洞 81 个（占 49%），其中互联网上出现“Bento4 内存泄露漏洞、 libming 内存泄露漏洞（CNVD-2024-48760）”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 36345 个，与上周（38375 个）环比减少 5%。

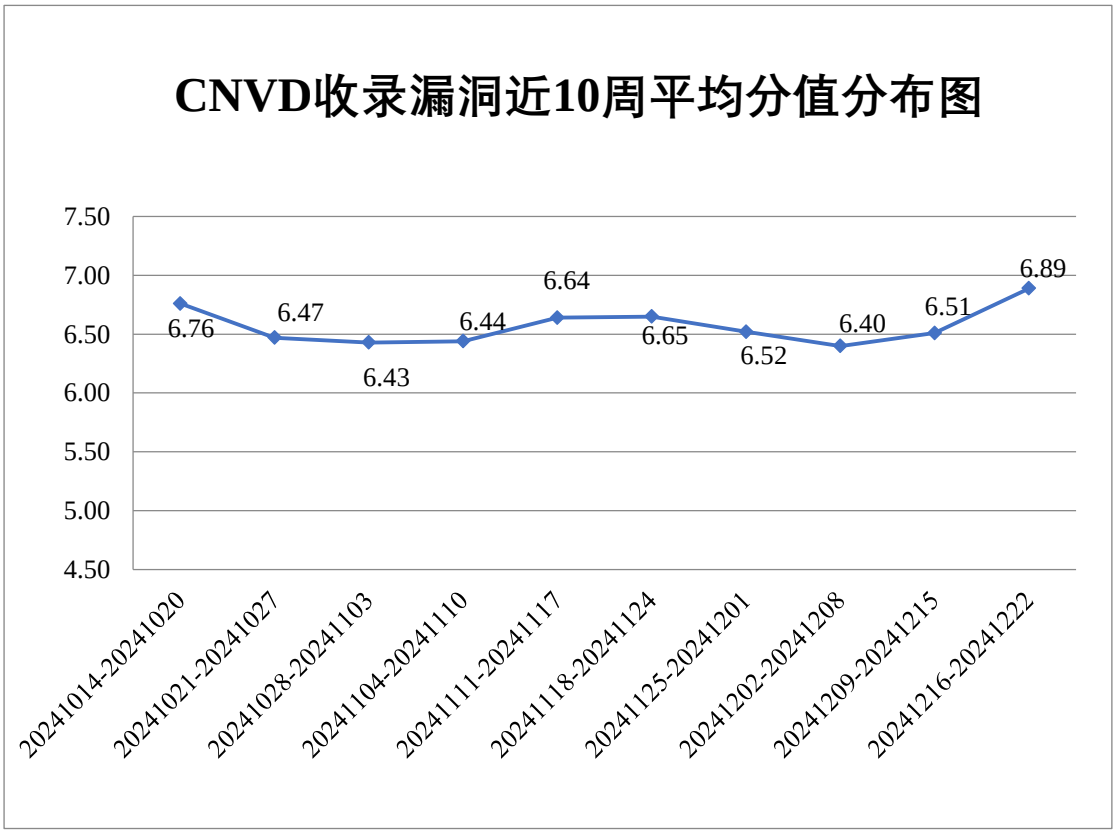

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 起，向基础电信企业通报漏洞事件 0 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 761 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 108 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 12 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：

中文在线集团股份有限公司、中卫信软件股份有限公司、智慧互通科技股份有限公司、正元智慧集团股份有限公司、浙江宇视科技有限公司、浙江兰德纵横网络技术股份有限公司、云南奇讯科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、夏普科技（上海）有限公司、武汉新致数字科技有限公司、武汉东信同邦信息技术有限公司、武汉达梦数据库有限公司、无锡信捷电气股份有限公司、卫宁健康科技集团股份有限公司、天津杏仁桉科技有限公司、天津天堰科技股份有限公司、天津环球磁卡集团有限公司、天地伟业技术有限公司、宿迁鑫潮信息技术有限公司、顺丰速运有限公司、神州数码控股有限公司、深圳亿玛信诺科技有限公司、深圳崖山科技有限公司、深圳市信锐网科技术有限公司、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、深圳达实智能股份有限公司、上海上讯信息技术股份有限公司、上海灵当信息科技有限公司、上海凯京信达科技集团有限公司、熵基科技股份有限公司、三星（中国）投资有限公司、若依、瑞斯康达科技发展股份有限公司、青岛海信网络科技股份有限公司、麒麟软件有限公司、罗技（中国）科技有限公司、老肯医疗科技股份有限公司、廊坊市极致网络科技有限公司、昆明阔驰科技公司、科大讯飞股份有限公司、柯尼卡美能达集团、佳能（中国）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、湖南华美信息系统有限公司、衡水金航计算机科技有限公司、合肥易用信息科技有限公司、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、杭州小海牛信息科技有限公司、杭州圣乔科技有限公司、杭州平治科技有限公司、杭州码里码外网络科技有限公司、杭州可道云网络有限公司、杭州海康威视数字技术股份有限公司、杭州短链网络技术有限公司、杭州安恒信息技术股份有限公司、哈尔滨伟成科技有限公司、广州红海云计算股份有限公司、广西方略网络技术有限公司、广联达科技股份有限公司、广东保伦电子股份有限公司、富士胶片商业创新（中国）有限公司、峰云物联科技有限公司、鼎点视讯科技有限公司、点都互联科技有限公司、大连华天软件有限公司、畅捷通信息技术股份有限公司、比亚迪股份有限公司、北京云帆互联科技有限公司、北京星网锐捷网络技术有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京神州视翰科技有限公司、北京灵州网络技术有限公司、北京理正软件股份有限公司、北京九思协同软件有限公司、北京镜舟

科技有限公司、北京金和网络股份有限公司、北京华夏春松科技有限公司、北京和欣运达科技有限公司、北京北大方正电子有限公司、奥琦玮信息科技（北京）有限公司和安科瑞电气股份有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、安天科技集团股份有限公司、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、杭州安恒信息技术股份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、江苏云天网络安全技术有限公司、交通运输信息安全中心有限公司、淮安易云科技有限公司、北京时代新威信息技术有限公司、国家计算机病毒应急处理中心、上海观安信息技术股份有限公司、北京天下信安技术有限公司、中国工商银行、河南东方云盾信息技术有限公司、江苏正信信息安全测试有限公司、天翼数字生活科技有限公司、江苏保旺达软件技术有限公司及其他个人白帽子向 CNVD 提交了 36345 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 35977 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）	20870	20870
奇安信网神（补天平台）	14646	14646
新华三技术有限公司	929	0
安天科技集团股份有限公司	523	0
北京天融信网络安全技术有限公司	452	8
北京神州绿盟科技有限公司	429	0
三六零数字安全科技集团有限公司	237	237
上海交大	224	224
杭州安恒信息技术股份有限公司	158	60
阿里云计算有限公司	144	0
京东科技信息技术有	122	5

限公司		
南京众智维信息科技有限公司	79	13
北京启明星辰信息安全技术有限公司	64	0
北京知道创宇信息技术有限公司	54	0
中国电信集团系统集成有限责任公司	42	0
北京安信天行科技有限公司	41	41
北京长亭科技有限公司	11	0
杭州迪普科技股份有限公司	10	0
北京纽盾网安信息技术有限公司	17	17
江苏云天网络安全技术有限公司	14	14
西门子（中国）有限公司	7	0
交通运输信息安全中心有限公司	6	6
淮安易云科技有限公司	4	4
北京时代新威信息技术有限公司	4	4
国家计算机病毒应急处理中心	1	1
上海观安信息技术股份有限公司	1	1
北京天下信安技术有限公司	1	1
中国工商银行	1	1
河南东方云盾信息技	1	1

术有限公司		
江苏正信信息安全测试有限公司	1	1
天翼数字生活科技有限公司	1	1
江苏保旺达软件技术有限公司	1	1
个人	188	188
报送总计	39283	36345

本周漏洞按类型和厂商统计

本周，CNVD 收录了 164 个漏洞。应用程序 67 个，WEB 应用 37 个，网络设备（交换机、路由器等网络端设备）34 个，操作系统 25 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
应用程序	67
WEB 应用	37
网络设备（交换机、路由器等网络端设备）	34
操作系统	25
数据库	1

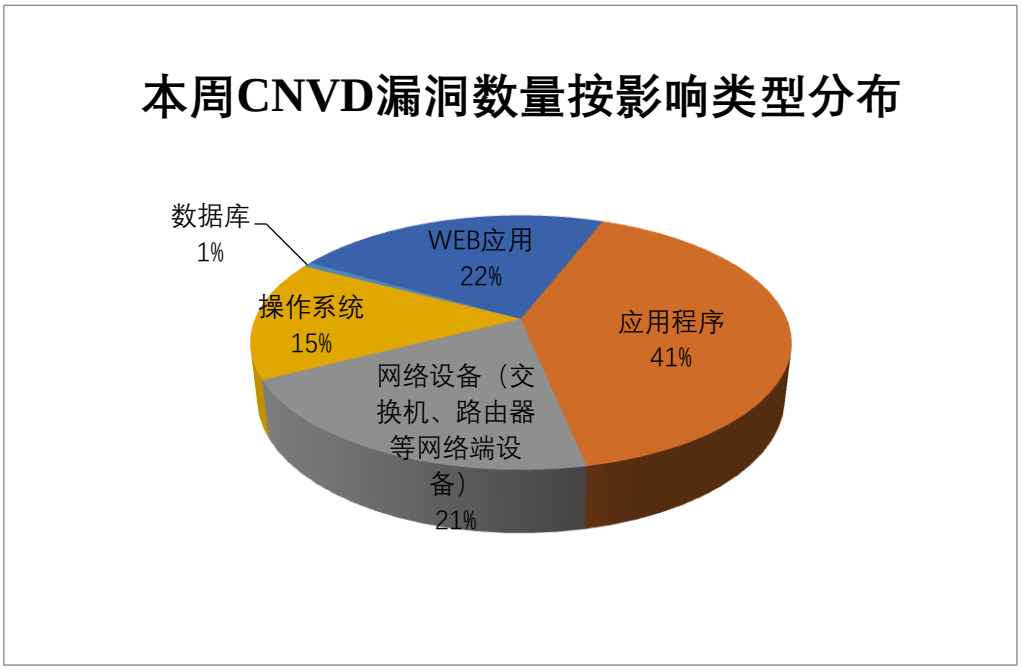

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、IrfanView 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	20	12%
2	Adobe	12	7%
3	IrfanView	10	6%
4	Mozilla	10	6%
5	Inductive Automation	8	5%
6	Apple	8	5%
7	ros-navigation	8	5%
8	Microsoft	8	5%
9	Siemens	7	4%
10	其他	73	45%

本周行业漏洞收录情况

本周，CNVD 收录了 8 个电信行业漏洞，16 个移动互联网行业漏洞，15 个工控行业漏洞（如下图所示）。其中，“Apache Tomcat 远程代码执行漏洞、Google Android 缓冲区溢出漏洞”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/

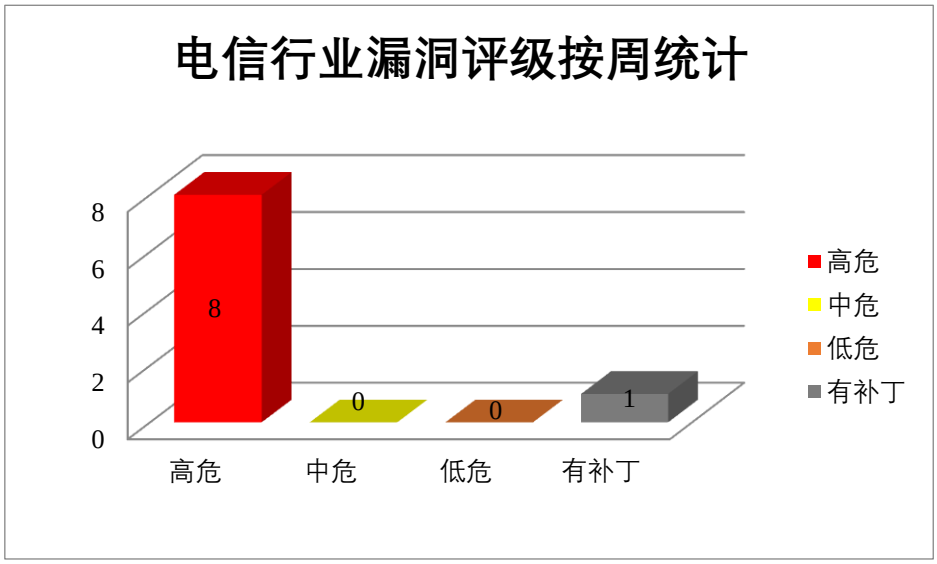

图 3 电信行业漏洞统计

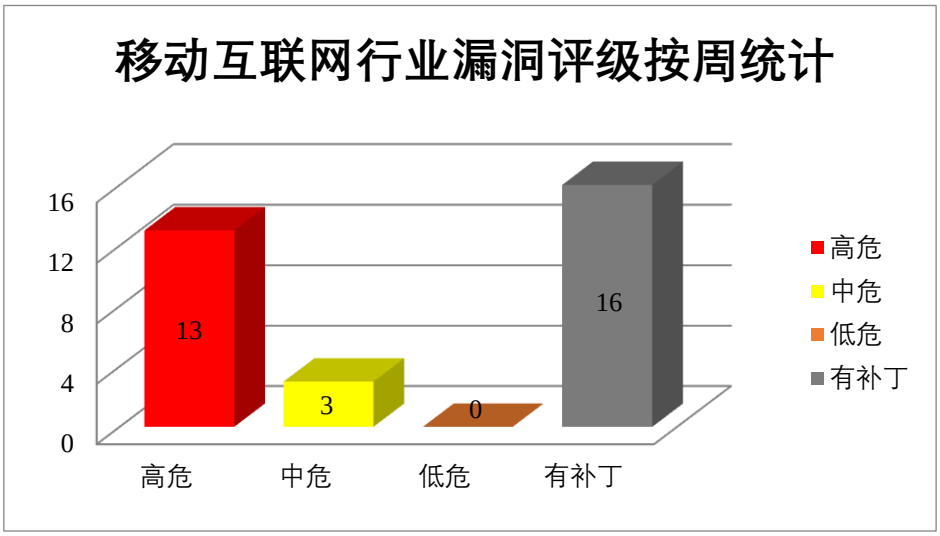

图 4 移动互联网行业漏洞统计

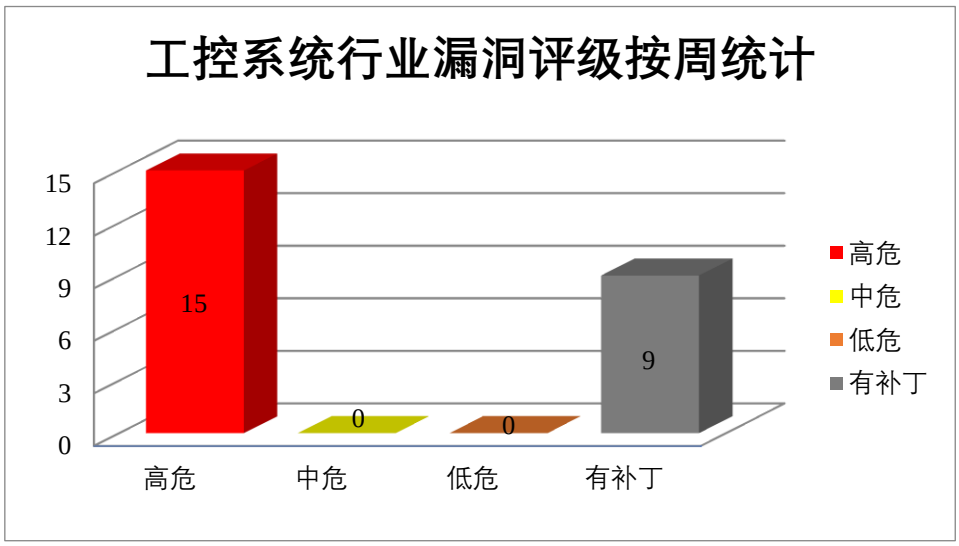

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。Microsoft Visual Studio Code 是美国微软（Microsoft）公司的一款开源的代码编辑器。Microsoft Visual Studio 是美国微软（Microsoft）公司的一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。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 SharePoint 权限提升漏洞（CNVD-2024-48

753）、Microsoft SharePoint 信息泄露漏洞（CNVD-2024-48752、CNVD-2024-48754）、Microsoft SharePoint 代码执行漏洞（CNVD-2024-48755、CNVD-2024-48756）、Microsoft Visual Studio Code Python Extension 远程代码执行漏洞、Microsoft Visual Studio Code extension for Arduino 远程代码执行漏洞、Microsoft Visual Studio 权限提升漏洞（CNVD-2024-48759）。其中，除“Microsoft SharePoint 信息泄露漏洞（CNVD-2024-48752）、Microsoft SharePoint 代码执行漏洞（CNVD-2024-48755）、Microsoft Visual Studio 权限提升漏洞（CNVD-2024-48759）”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-2024-48753

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48752

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48754

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48755

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48756

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48757

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48758

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48759

2、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。V8 是其中的一套开源 JavaScript 引擎。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，攻击者可利用漏洞导致越界写入，绕过安全限制，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 代码执行漏洞（CNVD-2024-48377、CNVD-2024-48376、CNVD-2024-48381、CNVD-2024-48383、CNVD-2024-48385）、Google Chrome 安全绕过漏洞（CNVD-2024-48382、CNVD-2024-48384）、Google Android 缓冲区溢出漏洞。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-2024-48377

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48376

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48382

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48381

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48384

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48383

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48385

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48772

3、 Adobe 产品安全漏洞

Adobe Substance 3D Painter 是美国奥多比（Adobe）公司的一个 3D 纹理处理应用程序。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 Substance 3D Painter 资源管理错误漏洞（CNVD-2024-48212）、Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-48216、CNVD-2024-48215、CNVD-2024-48214、CNVD-2024-48219、CNVD-2024-48218、CNVD-2024-48221、CNVD-2024-48220）。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-2024-48212
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48216
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48215
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48214
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48219
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48218
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48221
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48220

4、 Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox（Web 浏览器）的一个延长支持版本。Mozilla Thunderbird 是电子邮件客户端软件，支持 IMAP、POP 邮件协议以及 HTML 邮件格式。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浏览器崩溃，绕过下载保护，在易受攻击的系统上执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Mozilla 产品拒绝服务漏洞（CNVD-2024-48560）、多款 Mozilla 产品安全绕过漏洞（CNVD-2024-48561、CNVD-2024-48564）、多款 Mozilla 产品跨站脚本漏洞（CNVD-2024-48562）、多款 Mozilla 产品代码执行漏洞（CNVD-2024-48563）、多款 Mozilla 产品欺骗漏洞（CNVD-2024-48565）、Mozilla Firefox 安全绕过漏洞（CNVD-2024-48566）、Mozilla Firefox for iOS 欺骗漏洞。其中，除“多款 Mozilla 产品跨站脚本漏洞（CNVD-2024-48562）、多款 Mozilla 产品欺骗漏洞（CNVD-2024-48565）、Mozilla Firefox for iOS 欺骗漏洞”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-2024-48560
https://www.cnvd.org.cn/flaw/show/CNVD-2024-48561

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48562

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48563

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48564

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48565

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48566

https://www.cnvd.org.cn/flaw/show/CNVD-2024-48567

5、TOTOLINK X5000R 和 A7000R 缓冲区溢出漏洞

TOTOLINK X5000R 是一个路由器。TOTOLINK A7000R 是一款无线路由器。本周，TOTOLINK X5000R 和 A7000R 被披露存在缓冲区溢出漏洞，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-2024-48762

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-2024-48569	Mozilla Firefox 点击劫持漏洞（CNVD-2024-48569）	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://www.mozilla.org/en-US/security/advisories/mfsa2024-63/
CNVD-2024-48742	IrfanView DXF 文件解析类型混淆远程代码执行漏洞（CNVD-2024-48742）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.zerodayinitiative.com/advisories/ZDI-24-1603/
CNVD-2024-48744	IrfanView DWG 文件解析越界读取远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.zerodayinitiative.com/advisories/ZDI-24-1594/
CNVD-2024-48764	Inductive Automation Ignition 身份验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://inductiveautomation.com/blog/inductive-automation-participates-in-pwn2own-to-strengthen-ignition-security
CNVD-2024-48763	Inductive Automation Ignition OPC UA Quick Client 跨站脚本漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://inductiveautomation.com/blog/inductive-automation-participates-in-pwn2own-to-strengthen-ignition-secu

			rity
CNVD-2024-48766	Inductive Automation Ignition 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.inductiveautomation.com/hc/en-us/articles/7625759776653-Regarding-Pwn2Own-2022-Vulnerabilities
CNVD-2024-48765	Inductive Automation Ignition OPC UA Quick Client 任务调度远程代码执行漏洞	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://inductiveautomation.com/blog/inductive-automation-participates-in-pwn2own-to-strengthen-ignition-security
CNVD-2024-48768	Inductive Automation Ignition 访问控制错误漏洞	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://support.inductiveautomation.com/hc/en-us/articles/7625759776653-Regarding-Pwn2Own-2022-Vulnerabilities
CNVD-2024-48767	Inductive Automation Ignition 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：https://support.inductiveautomation.com/hc/en-us/articles/7625759776653-Regarding-Pwn2Own-2022-Vulnerabilities
CNVD-2024-48770	Inductive Automation Ignition 访问控制错误漏洞	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://support.inductiveautomation.com/hc/en-us/articles/7625759776653

小结：本周，Microsoft 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，在系统上执行任意代码等。此外，Google、Adobe、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致越界写入，绕过安全限制，在系统上执行任意代码等。另外，TOTOLINK X5000R 和 A7000R 被披露存在缓冲区溢出漏洞，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、 Bento4 内存泄露漏洞

验证描述

Bento4 是一款用于读写 MP4 文件的开源的 C++库。

Bento4 存在内存泄露漏洞，该漏洞源于 AP4_Movie::：AP4_Movie 未释放或无法释放已动态分配的堆内存，攻击者可利用该漏洞导致拒绝服务。

验证信息

POC 链接：https://github.com/axiomatic-systems/Bento4/issues/919

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-48761

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. Google 日历沦为钓鱼新工具，可绕过安全防护机制

根据 Check Point 与 Hackread.com 共同发布的最新研究报告，Google 工作空间中广泛应用的日程管理工具 Google 日历已成为网络犯罪分子的新攻击目标。

参考链接：https://hackread.com/google-calendar-phishing-scam-users-malicious-invites/

2. 黑客利用关键的 Fortinet EMS 漏洞部署远程访问工具

一个现已修补的影响 Fortinet FortiClient EMS 的关键安全漏洞正被恶意行为者利用，作为网络活动的一部分，安装了 AnyDesk 和 ScreenConnect 等远程桌面软件。

参考链接：https://thehackernews.com/2024/12/hackers-exploiting-critical-fortinet.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