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 02 日-2024 年 12 月 08 日 **2024 年第 49 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 377 个，其中高危漏洞 192 个、中危漏洞 155 个、低危漏洞 30 个。漏洞平均分值为 6.40。本周收录的漏洞中，涉及 0day 漏洞 275 个（占 73%），其中互联网上出现“MonoCMS 跨站脚本漏洞、厦门码英网络科技有限公司 MWCMS uploadeditor.html 页面文件上传漏洞”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 8839 个，与上周（3972 个）环比增加 123%。

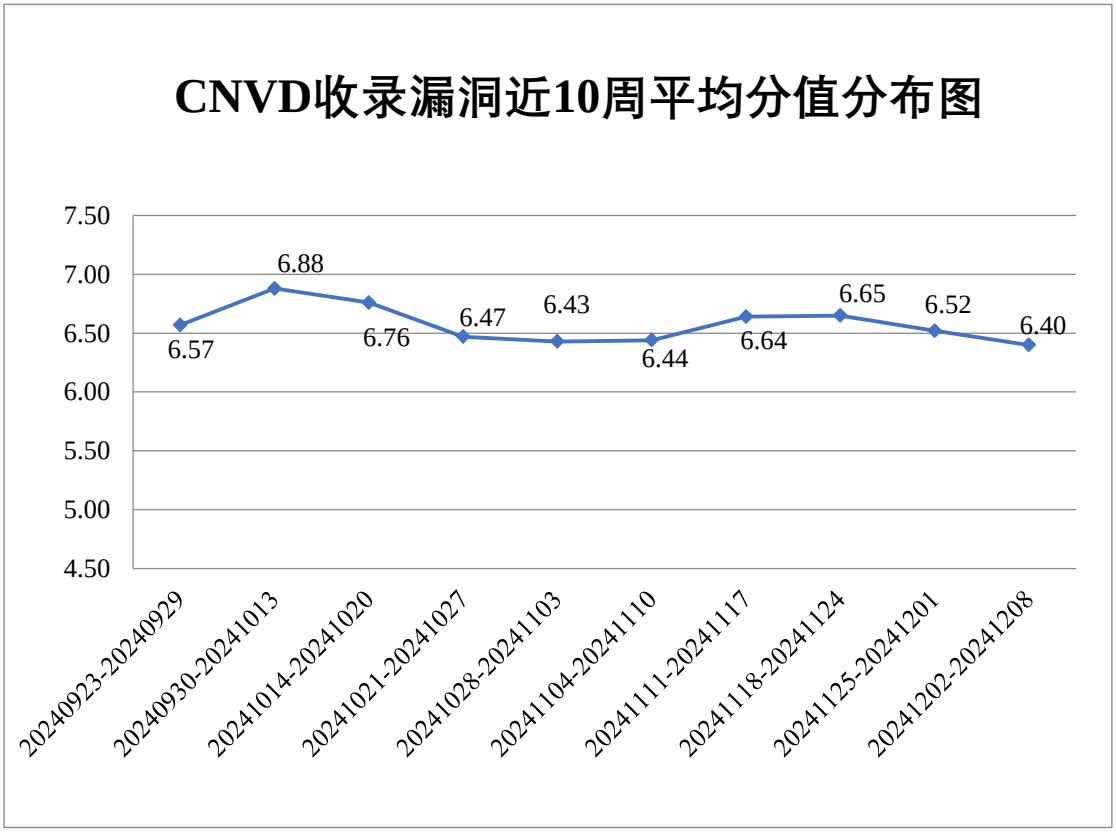

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 457 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 69 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 17 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、重庆光之际软件科技有限公司、中智贵阳人力资本科技有限公司、中新网络信息安全股份有限公司、中科方德软件有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、烟台海能仪表科技有限公司、信呼、新天科技股份有限公司、夏普商贸（中国）有限公司、武汉天地伟业科技有限公司、武汉烽火信息集成技术有限公司、微宏软件技术（杭州）有限公司、网是科技股份有限公司、统信软件技术有限公司、同望科技股份有限公司、天津神州浩天科技有限公司、天地伟业技术有限公司、四平市九州易通科技有限公司、四创科技有限公司、四川大家医学检测有限公司、神州数码控股有限公司、深圳益普科技有限公司、深圳拓安信物联股份有限公司、深圳市中控生物识别技术有限公司、深圳市有为信息技术发展有限公司、深圳市亿玛信诺科技有限公司、深圳市雄帝科技股份有限公司、深圳市网旭科技有限公司、深圳市同享软件科技有限公司、深圳市思迅软件股份有限公司、深圳市联软科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市汇川技术股份有限公司、深圳市必联电子有限公司、深圳勤杰软件有限公司、深圳安软信创技术有限公司、申瓯通信设备有限公司、上海曼恒数字技术股份有限公司、上海肯特仪表股份有限公司、上海互盾信息科技有限公司、上海泛微网络科技股份有限公司、上海博科资讯股份有限公司、厦门四信通信科技有限公司、容知日新科技股份有限公司、任子行网络技术股份有限公司、青果软件集团有限公司、青岛三利集团有限公司、青岛海信网络科技股份有限公司、青岛东胜伟业软件有限公司、麒麟软件有限公司、联想（北京）有限公司、蓝卓数字科技有限公司、可豪软件信息技术南京有限公司、柯尼卡美能达集团、凯特数智科技有限公司、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、合肥皖域信息科技有限公司、杭州云谷科技股份有限公司、杭州新中大科技股份有限公司、杭州圣乔科技有限公司、杭州立方控股股份有限公司、杭州海康威视数字技术股份有限公司、杭州冠航科技有限公司、杭州短链网络技术有限公司、哈尔滨新中新电子股份有限公司、广州致翔计算机科技有限公司、广州唯品会电子商务有限公司、广州同鑫科技有限公司、广州市保伦电子有限公司、广州红帆科技有限公司、广州高新兴机器人有限公司、广东顺景软件科技有限公司、广东保伦电子股份有限公司、高维数

据技术有限公司、富士胶片（中国）投资有限公司、大连华天软件有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、北京易成星光科技有限公司、北京亚控科技发展有限公司、北京熊宝贝科技发展有限公司、北京星网锐捷网络技术有限公司、北京小诗科技有限公司、北京网御星云信息技术有限公司、北京网易有道计算机系统有限公司、北京天拓四方科技股份有限公司、北京天融信网络安全技术有限公司、北京硕人时代科技股份有限公司、北京神州视翰科技有限公司、北京美特软件技术有限公司、北京龙软科技股份有限公司、北京灵州网络技术有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京慧点科技有限公司、北京宏景世纪软件股份有限公司、北京国网普瑞特高压输电技术有限公司、北京谷翔信息技术有限公司、北京北大方正电子有限公司、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、安元科技股份有限公司、安科瑞电气股份有限公司、安徽旭帆信息科技有限公司、安徽皖通邮电股份有限公司、安徽容知日新科技股份有限公司和漳州豆壳网络科技有限公司。

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、安天科技集团股份有限公司、北京神州绿盟科技有限公司、北京数字观星科技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、江苏保旺达软件技术有限公司、北京时代新威信息技术有限公司、淮安易云科技有限公司、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、北京山石网科信息技术有限公司、超聚变数字技术有限公司、上海观安信息技术股份有限公司、上海吨吨信息技术有限公司、国家计算机病毒应急处理中心、江苏云天网络安全技术有限公司、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及其他个人白帽子向 CNVD 提交了 4924 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（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 4544 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
奇安信网神（补天平台）	4060	4060
北京启明星辰信息安全技术有限公司	1254	0
新华三技术有限公司	740	0
安天科技集团股份有	433	0

限公司		
上海交大	465	465
北京神州绿盟科技有限公司	338	0
北京数字观星科技有限公司	320	0
深信服科技股份有限公司	284	0
阿里云计算有限公司	164	0
南京众智维信息科技有限公司	120	13
杭州安恒信息技术股份有限公司	100	0
北京知道创宇信息技术有限公司	98	0
北京天融信网络安全技术有限公司	61	8
远江盛邦（北京）网络安全科技股份有限公司	42	42
三六零数字安全科技集团有限公司	19	19
北京升鑫网络科技有限公司（青藤云）	17	17
中国电信集团系统集成有限责任公司	14	0
杭州迪普科技股份有限公司	10	0
快页信息技术有限公司	2	2
中孚安全技术有限公司	15	15
江苏保旺达软件技术有限公司	15	15
北京时代新威信息技	6	6

术有限公司		
淮安易云科技有限公司	5	5
河南东方云盾信息技术有限公司	4	4
江苏正信信息安全测试有限公司	3	3
北京山石网科信息技术有限公司	3	3
超聚变数字技术有限公司	2	2
上海观安信息技术股份有限公司	2	2
上海吨吨信息技术有限公司	1	1
国家计算机病毒应急处理中心	1	1
江苏云天网络安全技术有限公司	1	1
上海亿保健康科技集团有限公司	1	1
北京卓识网安技术股份有限公司	1	1
CNCERT 河南分中心	3	3
CNCERT 贵州分中心	1	1
个人	234	234
报送总计	8839	4924

本周漏洞按类型和厂商统计

本周，CNVD 收录了 377 个漏洞。WEB 应用 211 个，应用程序 97 个，网络设备（交换机、路由器等网络端设备）40 个，智能设备（物联网终端设备）17 个，安全产品 5 个，数据库 4 个，操作系统 3 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	211
应用程序	97
网络设备（交换机、路由器等网络端设备）	40
智能设备（物联网终端设备）	17
安全产品	5
数据库	4
操作系统	3

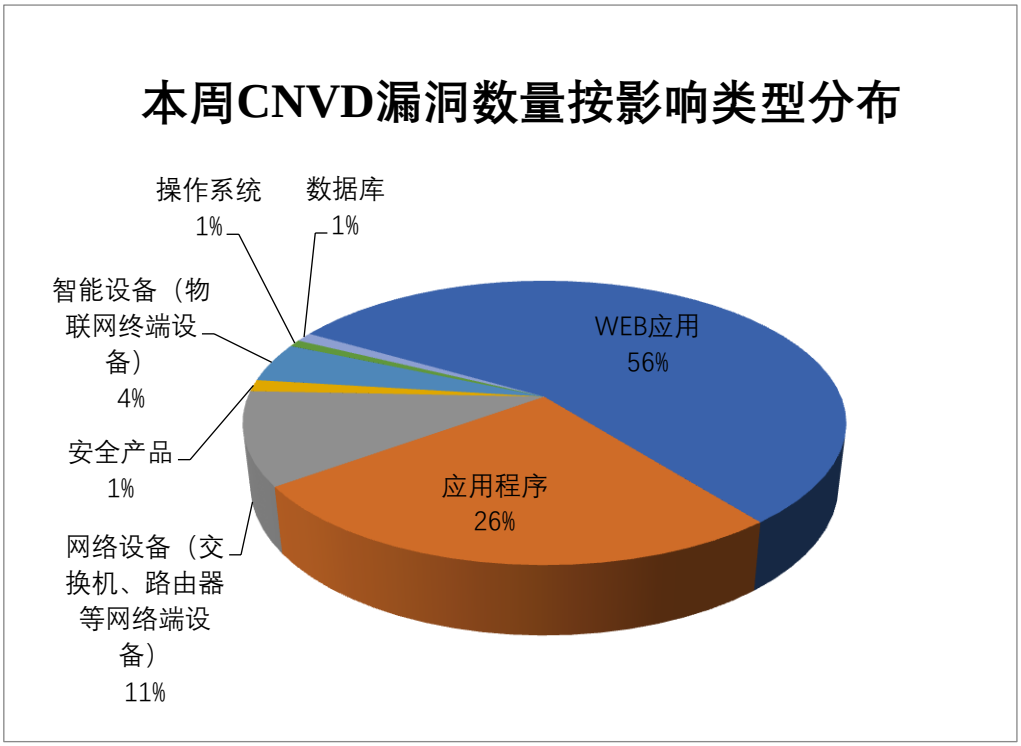

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IrfanView、畅捷通信息技术股份有限公司、IBM 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	IrfanView	27	7%
2	畅捷通信息技术股份有限公司	15	3%
3	IBM	11	3%
4	Adobe	11	3%
5	北京神州视翰科技有限公司	11	3%
6	Rockwell Automation	11	3%
7	北京亿赛通科技发展有限责任公司	10	3%
8	广东保伦电子股份有限公	10	3%

	司		
9	用友网络科技股份有限公司	10	3%
10	其他	261	69%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，3 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，“NETGEAR XR300 genie_dyn.cgi 组件命令注入漏洞、Google Android 权限提升漏洞（CNVD-2024-47284）”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/

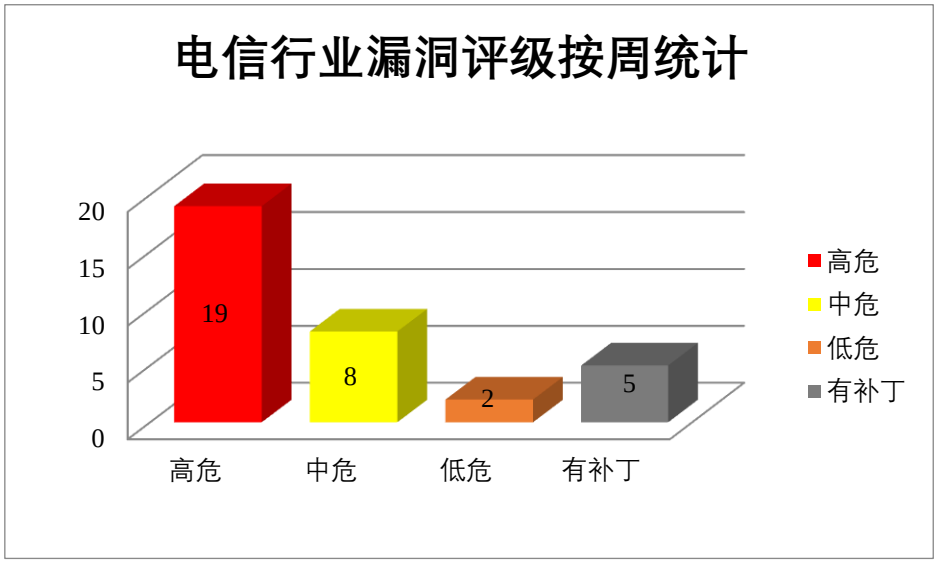

图 3 电信行业漏洞统计

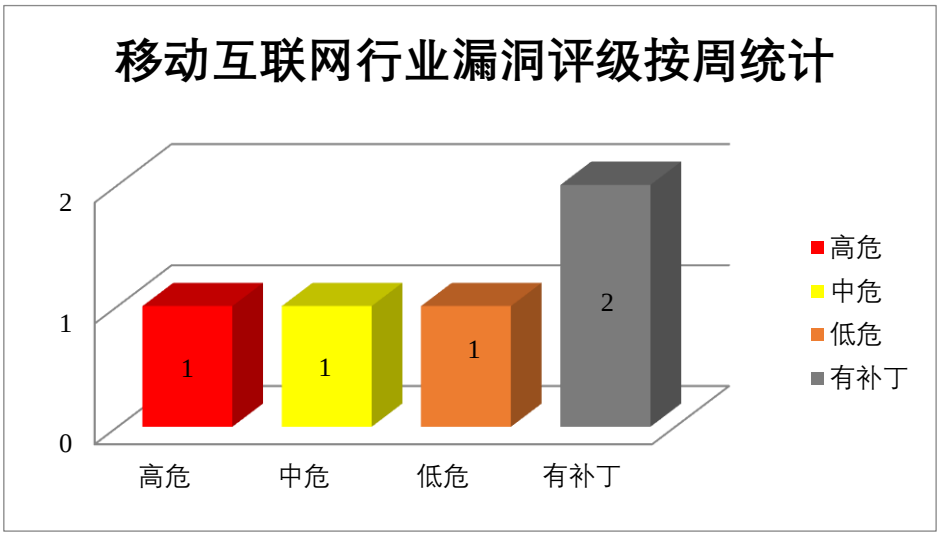

图 4 移动互联网行业漏洞统计

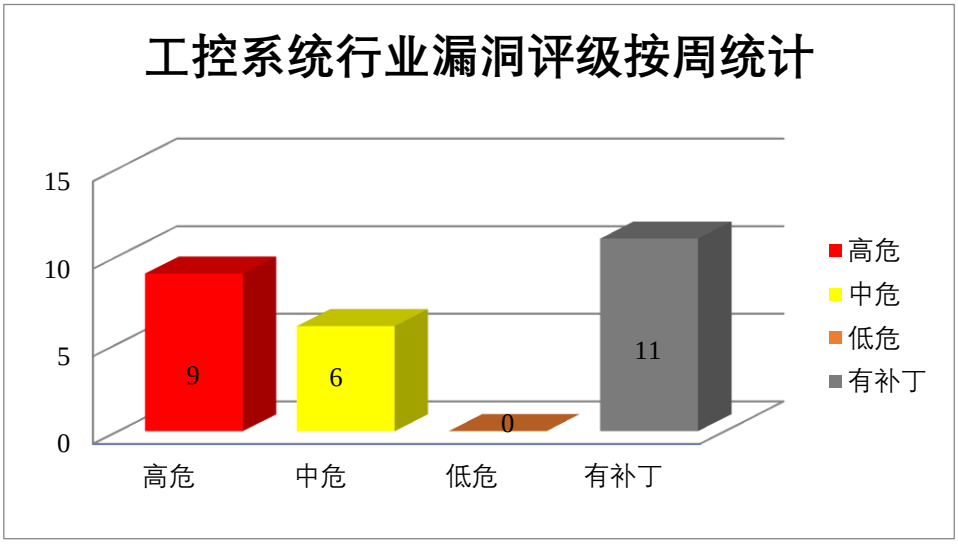

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Concert 是美国国际商业机器（IBM）公司的一种新工具。使用生成式 AI 来帮助管理复杂的云原生应用程序。IBM Security SOAR 是美国国际商业机器（IBM）公司的一款产品，前身为 Resilient。旨在帮助您的安全团队自信地应对网络威胁、通过智能实现自动化并通过一致性进行协作。IBM CICS TX Standard 是美国国际商业机器(IBM)公司的一个综合的单一事务运行时包，可以为独立应用程序提供云原生部署模型。IBM WebSphere Application Server（WAS）是美国国际商业机器（IBM）公司的一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。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，发送特制的 SQL 语句，从而查看、添加、修改或删除后端数据库中的信息，绕过 Web 身份验证并获得设备的管理访问权限等。

CNVD 收录的相关漏洞包括：IBM Concert 加密问题漏洞、IBM Concert SQL 注入漏洞、IBM Concert 跨站脚本漏洞（CNVD-2024-46794）、IBM Security SOAR 授权问题漏洞、IBM Concert 访问控制错误漏洞、IBM CICS TX Standard Web UI 跨站请求伪造漏洞、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2024-46815）、IBM CICS TX Standard Web UI 跨站脚本漏洞。其中，“IBM Concert SQL 注入漏洞、IBM Security SOAR 授权问题漏洞、IBM CICS TX Standard Web UI 跨站请求伪造漏洞”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-2024-46793
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46795
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46794
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46797
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46796
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46813
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46815
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46814

2、 Adobe 产品安全漏洞

Adobe After Effects 是美国奥多比（Adobe）公司的一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。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 Commerce 是一个单一的多渠道商务平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致敏感内存泄露，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe After Effects 缓冲区溢出漏洞（CNVD-2024-46798、CNVD-2024-46799、CNVD-2024-46800、CNVD-2024-46803）、Adobe Animate 缓冲区溢出漏洞（CNVD-2024-46804）、Adobe Illustrato 缓冲区溢出漏洞（CNVD-2024-46807）、Adobe Animate 资源管理错误漏洞（CNVD-2024-46806）、Adobe Commerce 缓冲区溢出漏洞。其中，除“Adobe After Effects 缓冲区溢出漏洞（CNVD-2024-46798）”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-2024-46798
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46799
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46800
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46803
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46804
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46807
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46806
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46820

3、 Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox（Web 浏览器）的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。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跨源 JSON 内容，绕过安全限制，在易受攻击的系统上执行任意代码或造成拒

绝服务。

CNVD 收录的相关漏洞包括：多款 Mozilla 产品安全绕过漏洞（CNVD-2024-46832、CNVD-2024-46829）、多款 Mozilla 产品信息泄露漏洞（CNVD-2024-46831、CNVD-2024-46834）、多款 Mozilla 产品代码执行漏洞（CNVD-2024-46833、CNVD-2024-46836、CNVD-2024-46830）、多款 Mozilla 产品欺骗漏洞（CNVD-2024-46835）。其中，除“多款 Mozilla 产品安全绕过漏洞（CNVD-2024-46829）”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-2024-46829

https://www.cnvd.org.cn/flaw/show/CNVD-2024-46831

https://www.cnvd.org.cn/flaw/show/CNVD-2024-46830

https://www.cnvd.org.cn/flaw/show/CNVD-2024-46832

https://www.cnvd.org.cn/flaw/show/CNVD-2024-46834

https://www.cnvd.org.cn/flaw/show/CNVD-2024-46833

https://www.cnvd.org.cn/flaw/show/CNVD-2024-46836

https://www.cnvd.org.cn/flaw/show/CNVD-2024-46835

4、 Rockwell Automation 产品安全漏洞

Rockwell Automation ThinManager 是美国罗克韦尔（Rockwell Automation）公司的一款瘦客户端管理软件。允许将瘦客户端同时分配给多个远程桌面服务器。Rockwell Automation FactoryTalk View Site Edition 是美国罗克韦尔（Rockwell Automation）公司的一个集成软件包。用于开发和运行。Rockwell Automation 5015-U8IHFT 是美国罗克韦尔（Rockwell Automation）公司的一个通用模块。Rockwell Automation Sequence Manager 是美国罗克韦尔（Rockwell Automation）公司的一个基于控制器的基本批处理管理。Rockwell Automation PowerFlex 6000T 是美国罗克韦尔（Rockwell Automation）公司的一款中压变频器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞向设备发送特制的消息，导致拒绝服务，提交特殊的请求，上传恶意文件，在应用程序上下文执行任意代码等。

CNVD 收录的相关漏洞包括：Rockwell Automation ThinManager 身份验证错误漏洞、Rockwell Automation FactoryTalk View Site Edition 远程代码执行漏洞、Rockwell Automation 5015-U8IHFT 拒绝服务漏洞、Rockwell Automation SequenceManager 输入验证错误漏洞、Rockwell Automation PowerFlex 6000T 拒绝服务漏洞、Rockwell Automation ThinManager 拒绝服务漏洞、Rockwell Automation ThinManager ThinServer 远程代码执行漏洞、Rockwell Automation ThinManager 输入验证错误漏洞。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-2024-46725
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46730
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46729
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46728
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46727
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46726
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46735
https://www.cnvd.org.cn/flaw/show/CNVD-2024-46731

5、TP-LINK TL-WDR7660 rtRuleJsonTobin 函数缓冲区溢出漏洞

TP-LINK TL-WDR7660 是中国普联（TP-LINK）公司的一款千兆路由器。本周，TP-LINK TL-WDR7660 被披露存在缓冲区溢出漏洞。攻击者可以利用该漏洞在系统上执行任意代码或者导致拒绝服务攻击。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-2024-47286

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-2024-46824	IrfanView WBZ 插件 WB1 文件解析越界写入远程代码执行漏洞	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-24-1555/
CNVD-2024-46823	IrfanView DXF 文件解析类型混淆远程代码执行漏洞	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-24-1604/
CNVD-2024-46826	IrfanView PSP 文件解析越界写入远程代码执行漏洞（CNVD-2024-46826）	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-24-971/
CNVD-2024-46825	IrfanView WBZ 插件 WB1 堆栈文件解析缓冲区溢出远程代码执行漏洞	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-24-1557/
CNVD-2024-46828	IrfanView PSP 文件解析越界写入远程代码执行漏洞	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.zerodayinitiative.com/advisories/ZDI-24-970/

CNVD-2024-46827	IrfanView CIN 文件解析越界写入远程代码执行漏洞	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-24-974/
CNVD-2024-47201	IrfanView 越界写入漏洞（CNVD-2024-47201）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.irfanview.com/
CNVD-2024-47203	IrfanView 越界写入漏洞（CNVD-2024-47203）	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.irfanview.com/
CNVD-2024-47202	IrfanView 越界写入漏洞（CNVD-2024-47202）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.irfanview.com/
CNVD-2024-47204	IrfanView 越界读取漏洞（CNVD-2024-47204）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.irfanview.com/

小结：本周，IBM 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，发送特制的 SQL 语句，从而查看、添加、修改或删除后端数据库中的信息，绕过 Web 身份验证并获得设备的管理访问权限。此外，Adobe、Mozilla、Rockwell Automation 等多款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等。另外，TP-LINK TL-WDR7660 被披露存在缓冲区溢出漏洞。攻击者可以利用该漏洞在系统上执行任意代码或者导致拒绝服务攻击。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、MonoCMS 跨站脚本漏洞

验证描述

MonoCMS 是一个免费的开源内容管理系统。

MonoCMS /monofiles/opensaved.php 处理 filtcategory 参数存在跨站脚本漏洞，远程攻击者可利用该漏洞注入恶意脚本或 HTML 代码，当恶意数据被查看时，可获取敏感信息或劫持用户会话。

验证信息

POC 链接：https://github.com/secuserx/CVE/blob/main/%5BXSS%20vulnerability%5D%20found%20in%20MonoCMS%2023-20240528%20-%20(opensaved.php).md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-46808

信息提供者

北京启明星辰信息安全技术有限公司

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. I-O Data 路由器 0Day 漏洞被利用，无修复补丁

日本计算机紧急响应小组（CERT）警告称，黑客正在利用 I-O Data 路由器设备中的零日漏洞来修改设备设置、执行命令，甚至关闭防火墙。

参考链接：https://www.bleepingcomputer.com/news/security/japan-warns-of-io-data-zero-day-router-flaws-exploited-in-attacks/

2. 最强大的 Android 间谍软件曝光，可提取信息、密码和执行 shell 命令

该恶意软件似乎是 Monokle 的新版本，Monokle 最初由 Lookout 在 2019 年发现，由总部位于圣彼得堡的特种技术中心有限公司开发。

参考链接：https://www.bleepingcomputer.com/news/security/new-android-spyware-found-on-phone-seized-by-russian-fsb/

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