国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 01 月 22 日-2024 年 01 月 28 日 **2024 年第 4 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 406 个，其中高危漏洞 185 个、中危漏洞 209 个、低危漏洞 12 个。漏洞平均分值为 6.50。本周收录的漏洞中，涉及 0day 漏洞 316 个（占 78%），其中互联网上出现“SeaCMS 跨站脚本漏洞（CNVD-2024-06149）、江西铭软科技有限公司 MCMS SQL 注入漏洞”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事件型漏洞总数 12980 个，与上周（4975 个）环比增加 1.61 倍。

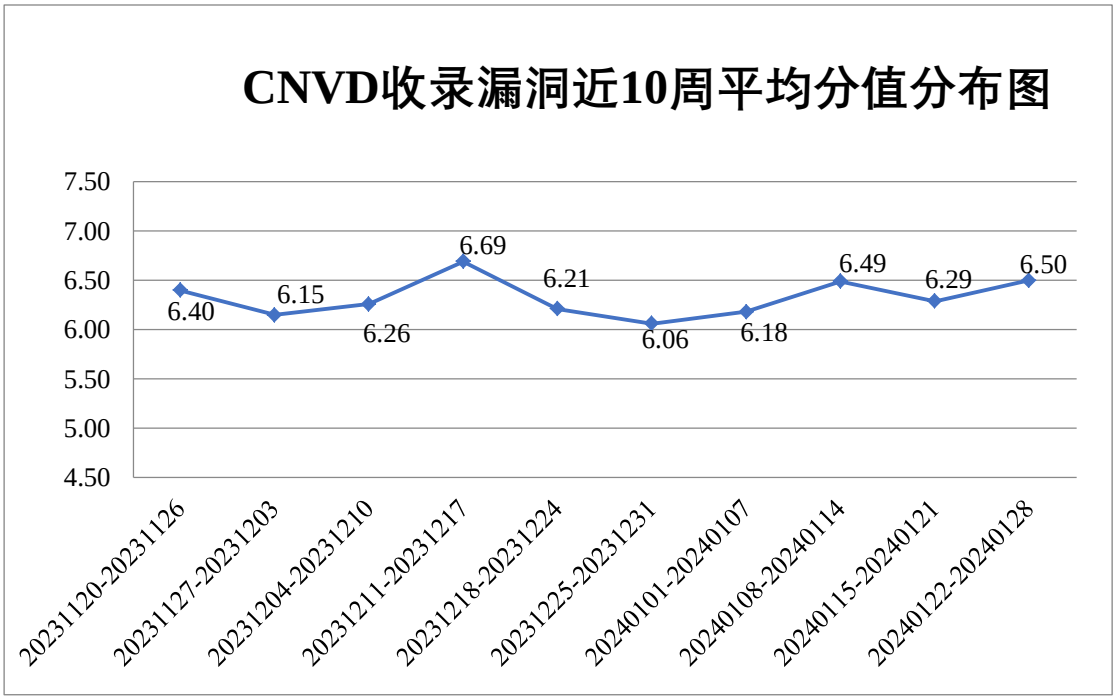

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 13 起，向基础电

信企业通报漏洞事件 8 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 632 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 57 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 32 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：

珠海金山办公软件有限公司、长沙友点软件科技有限公司、昱能科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、研华科技（中国）有限公司、西安瑞友信息技术资讯有限公司、无锡路通视信网络股份有限公司、潍坊家园驿站电子技术有限公司、威博通科技（上海）有限公司、天地（常州）自动化股份有限公司、苏州真趣信息科技有限公司、苏州科达科技股份有限公司、思科系统（中国）网络技术有限公司、世邦通信股份有限公司、师创教育软件研究院（江苏）有限公司、深圳市普燃计算机软件科技有限公司、深圳市明源云科技有限公司、深圳市美科星通信技术有限公司、深圳市绿联科技股份有限公司、深圳市磊科实业有限公司、深圳市蓝凌软件股份有限公司、深圳市科图自动化新技术有限公司、深圳市吉祥腾达科技有限公司、上汽大通汽车销售服务有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海注亿科技有限公司、上海司南卫星导航技术股份有限公司、上海普华科技发展股份有限公司、上海穆云智能科技有限公司、上海建文软件有限公司、上海寰创通信科技股份有限公司、上海亘岩网络科技有限公司、上海顶想信息科技有限公司、上海布雷德科技有限公司、上海艾泰科技有限公司、山石网科通信技术股份有限公司、三星（中国）投资有限公司、群晖科技股份有限公司、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、南京数旗科技有限公司、南京纳龙科技有限公司、龙芯中科技术股份有限公司、龙采科技集团有限责任公司、廊坊市极致网络科技有限公司、蓝网科技股份有限公司、金蝶软件（中国）有限公司、江苏慧泽信息技术有限公司、吉翁电子（深圳）有限公司、惠尔丰信息系统有限公司、湖南奥科网络技术股份有限公司、河北微引擎网络科技有限公司、杭州有赞科技有限公司、杭州盈高科技有限公司、杭州九麒科技有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、哈尔滨新中新电子股份有限公司、广州拓波软件科技有限公司、广州市可视智能技术有限公司、广州华壹智能科技有限公司、广东飞企互联科技股份有限公司、富士施乐（中国）有限公司、富士胶片商业创新（中国）有限公司、福州银达云创信息科技有限公司、福建科立讯通信有限公司、帝国软件、大唐电信科技股份有限公司、成都德芯数字科技股份有限公司、北京卓软在线信息技术有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京清科锐华软件有限公司、北京清大新洋科技有限公司、北京灵州网络技术有限公司、北京兰德华电子技术有限公司、北京康比特体育科技股份有限公司、北京金自天正智能控制股份有限公司、北京慧点科技有限公司、北京格林威尔科技发展有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限

公司、安徽蓝盾光电子股份有限公司、ZZCMS 和 NEC。

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、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、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。江苏金盾检测技术股份有限公司、贵州多彩网安科技有限公司、快页信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、联想集团、北京卓识网安技术股份有限公司、安全邦（北京）信息技术有限公司、中国电信股份有限公司上海研究院、内蒙古洞明科技有限公司、任子行网络技术股份有限公司、亚信科技（成都）有限公司、四川赛闯检测股份有限公司、湖南泛联新安信息科技有限公司、山石网科通信技术股份有限公司、北京山石网科信息技术有限公司、上海直画科技有限公司、江苏极元信息技术有限公司、北京天防安全科技有限公司、中孚安全技术有限公司、南京先维信息技术有限公司、安徽锋刃信息科技有限公司、杭州默安科技有限公司、江苏云天网络安全技术有限公司、江苏百达智慧网络科技有限公司、北京安华金和科技有限公司、深圳昂楷科技有限公司、安徽天行网安信息安全技术有限公司、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、河南灵创电子科技有限公司、河南悦海数安科技有限公司、平安银河实验室、甘肃赛飞安全科技有限公司、湖南省电子信息产业研究院、中国工商银行、江苏网擎信息技术有限公司、成都愚安科技有限公司、广州安亿信软件科技有限公司、赛尔网络有限公司及其他个人白帽子向 CNVD 提交了 12980 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 11033 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
斗象科技（漏洞盒子）	8870	8870
奇安信网神（补天平台）	1029	1029
三六零数字安全科技集团有限公司	779	779
新华三技术有限公司	778	0
北京天融信网络安全技术有限公司	764	3
北京神州绿盟科技有	478	0

限公司		
深信服科技股份有限公司	360	0
安天科技集团股份有限公司	360	0
北京数字观星科技有限公司	355	0
上海交大	355	355
阿里云计算有限公司	269	6
中国电信集团系统集成有限责任公司	140	0
杭州安恒信息技术股份有限公司	97	48
北京启明星辰信息安全技术有限公司	94	24
北京知道创宇信息技术有限公司	70	9
恒安嘉新（北京）科技股份公司	35	0
北京长亭科技有限公司	30	10
北京安信天行科技有限公司	12	12
北京智游网安科技有限公司	2	2
西安四叶草信息技术有限公司	2	2
南京联成科技发展股份有限公司	1	1
厦门服云信息科技有限公司	1	1
江苏金盾检测技术股份有限公司	44	44
贵州多彩网安科技有限公司	43	43

快页信息技术有限公司	32	32
奇安星城网络安全运营服务（长沙）有限公司	31	31
河南东方云盾信息技术有限公司	29	29
联想集团	27	27
北京卓识网安技术股份有限公司	13	13
安全邦（北京）信息技术有限公司	11	11
中国电信股份有限公司上海研究院	8	8
内蒙古洞明科技有限公司	8	8
任子行网络技术股份有限公司	8	8
亚信科技（成都）有限公司	7	7
四川赛闯检测股份有限公司	7	7
湖南泛联新安信息科技有限公司	7	7
山石网科通信技术股份有限公司	7	7
北京山石网科信息技术有限公司	6	6
上海直画科技有限公司	6	6
江苏极元信息技术有限公司	6	6
北京天防安全科技有限公司	5	5
中孚安全技术有限公	5	5

司		
南京先维信息技术有限公司	4	4
安徽锋刃信息科技有限公司	4	4
杭州默安科技有限公司	4	4
江苏云天网络安全技术有限公司	3	3
江苏百达智慧网络科技有限公司	3	3
北京安华金和科技有限公司	2	2
深圳昂楷科技有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2
北京天下信安技术有限公司	2	2
苏州棱镜七彩信息科技有限公司	1	1
河南灵创电子科技有限公司	1	1
河南悦海数安科技有限公司	1	1
平安银河实验室	1	1
甘肃赛飞安全科技有限公司	1	1
湖南省电子信息产业研究院	1	1
中国工商银行	1	1
江苏网擎信息技术有限公司	1	1
成都愚安科技有限公司	1	1

广州安亿信软件科技有限公司	1	1
赛尔网络有限公司	1	1
个人	1482	1482
报送总计	16710	12980

本周漏洞按类型和厂商统计

本周，CNVD 收录了 406 个漏洞。WEB 应用 212 个，网络设备（交换机、路由器等网络端设备）85 个，应用程序 72 个，操作系统 15 个，智能设备（物联网终端设备）12 个，安全产品 8 个，数据库 1 个，车联网 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	212
网络设备（交换机、路由器等网络端设备）	85
应用程序	72
操作系统	15
智能设备（物联网终端设备）	12
安全产品	8
数据库	1
车联网	1

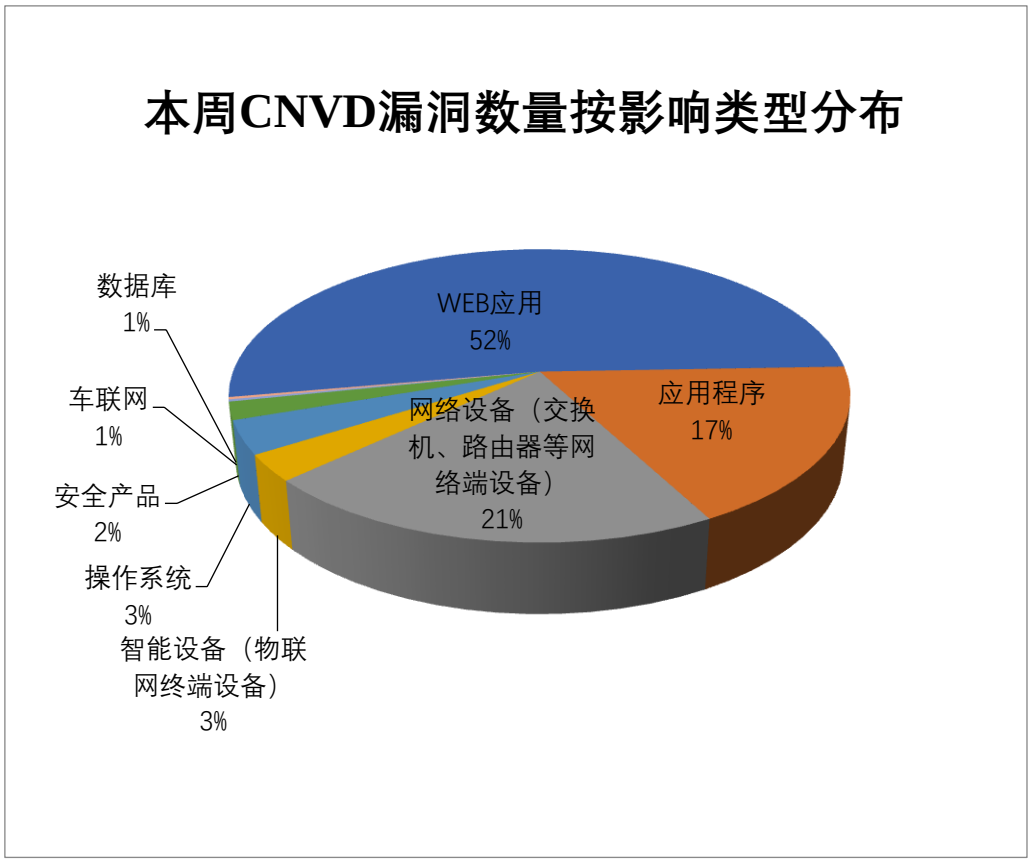

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Tenda、北京亿赛通科技发展有限责任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	D-Link	24	6%
2	Tenda	14	4%
3	北京亿赛通科技发展有限责任公司	14	4%
4	用友网络科技股份有限公司	11	3%
5	Google	11	3%
6	北京百卓网络技术有限公司	11	3%
7	Adobe	10	2%
8	Trend Micro	10	2%
9	珠海金山办公软件有限公司	9	2%
10	其他	292	71%

本周行业漏洞收录情况

本周，CNVD 收录了 51 个电信行业漏洞，31 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Tenda AX1803 命令注入漏洞、Google Android 权限提升漏洞（CNVD-2024-05386）”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/

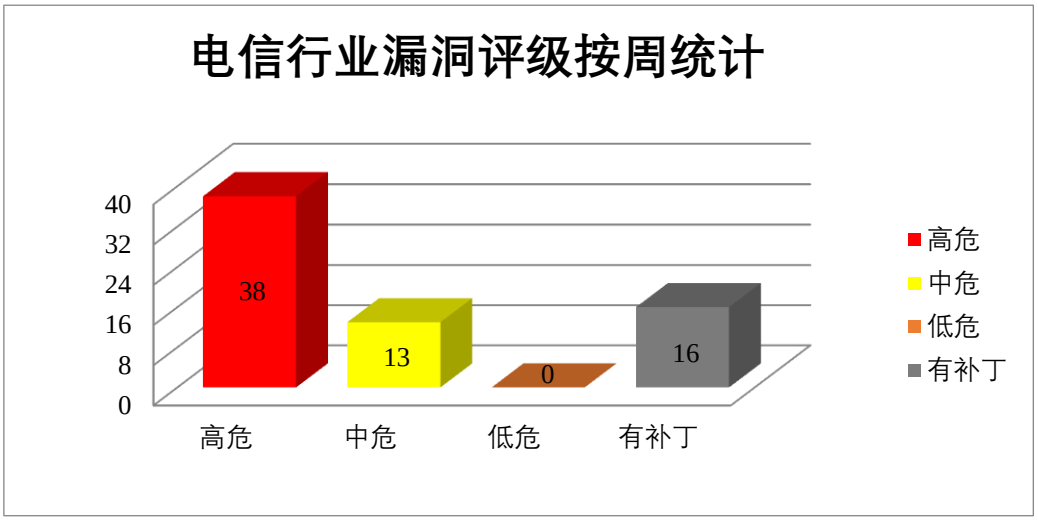

图 3 电信行业漏洞统计

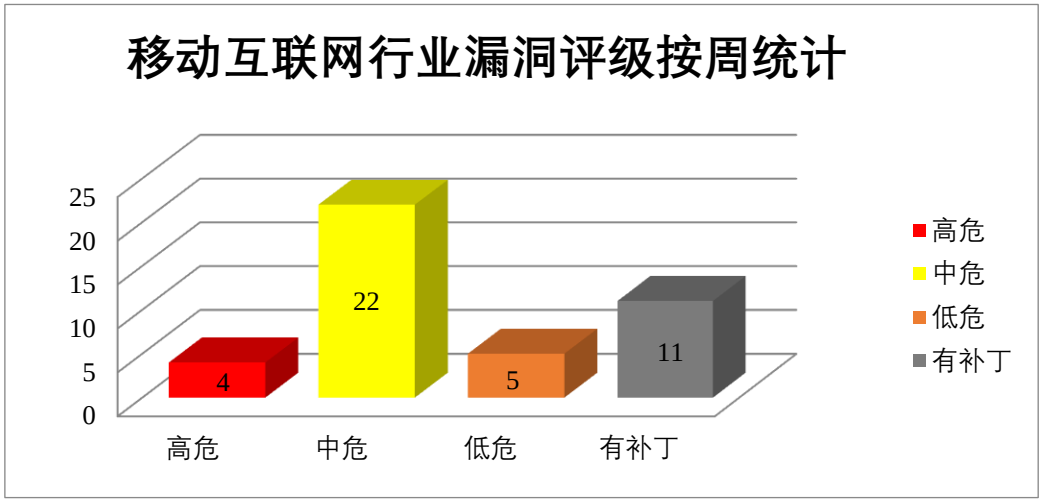

图 4 移动互联网行业漏洞统计

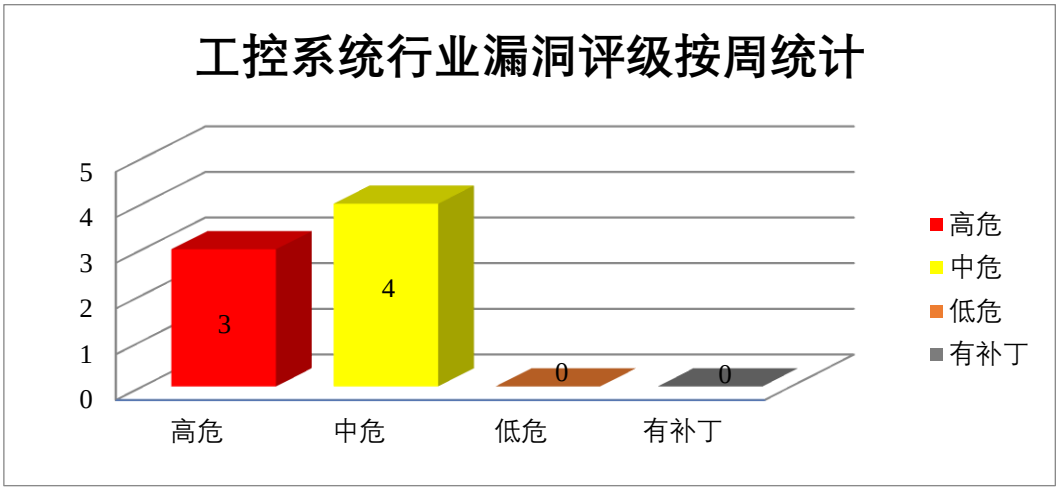

图 5 工控系统行业漏洞统计

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、D-Link 产品安全漏洞

D-Link DIR-823G 是中国友讯（D-Link）公司的一款无线路由器。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞导致拒绝服务。

CNVD 收录的相关漏洞包括：D-Link DIR-823G 缓冲区溢出漏洞（CNVD-2024-04955）、D-Link DIR-823G SetDeviceSettings 函数缓冲区溢出漏洞、D-Link DIR-823G EndTime 参数缓冲区溢出漏洞、D-Link DIR-823G Mac 参数缓冲区溢出漏洞、D-Link DIR-823G StartTime 参数缓冲区溢出漏洞、D-Link DIR-823G MacAddress 参数缓冲区溢出漏洞、D-Link DIR-823G Password 参数缓冲区溢出漏洞、D-Link DIR-823G Encryption 参数缓冲区溢出漏洞。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-2024-04955
https://www.cnvd.org.cn/flaw/show/CNVD-2024-05331
https://www.cnvd.org.cn/flaw/show/CNVD-2024-05332
https://www.cnvd.org.cn/flaw/show/CNVD-2024-05333
https://www.cnvd.org.cn/flaw/show/CNVD-2024-05334
https://www.cnvd.org.cn/flaw/show/CNVD-2024-05335
https://www.cnvd.org.cn/flaw/show/CNVD-2024-05336
https://www.cnvd.org.cn/flaw/show/CNVD-2024-05337

2、Microsoft 产品安全漏洞

Microsoft Message Queuing 是用于实现需要高性能的异步和同步场景的解决方案。

本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从堆内存中获取敏感信息，在系统上执行任意代码，导致系统拒绝服务。

CNVD 收录的相关漏洞包括：Microsoft Message Queuing 拒绝服务漏洞（CNVD-2024-04948、CNVD-2024-04952）、Microsoft Message Queuing 信息泄露漏洞（CNVD-2024-04947、CNVD-2024-04946、CNVD-2024-04950、CNVD-2024-04949、CNVD-2024-04951）、Microsoft Message Queuing 远程代码执行漏洞（CNVD-2024-04953）。其中，“Microsoft Message Queuing 拒绝服务漏洞（CNVD-2024-04948、CNVD-2024-04952）、Microsoft Message Queuing 远程代码执行漏洞（CNVD-2024-04953）”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-2024-04948
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04947
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04946
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04950
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04949
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04952
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04951
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04953

3、Trend Micro 产品安全漏洞

Trend Micro Apex Central 是美国趋势科技(Trend Micro)公司的一个基于 Web 的产品控制台。Trend Micro Apex One 是一套能够提供自动威胁检测和响应功能的端点安全防护软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞注入恶意脚本或 HTML 代码，提升权限，在系统上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Trend Micro Apex Central 本地文件包含漏洞、Trend Micro Apex Central 跨站脚本漏洞（CNVD-2024-04936、CNVD-2024-04937）、Trend Micro Apex One 权限提升漏洞（CNVD-2024-04943、CNVD-2024-04942、CNVD-2024-04941、CNVD-2024-04945、CNVD-2024-04944）。其中，“Trend Micro Apex Central 本地文件包含漏洞”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-2024-04936
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04940
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04937
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04943
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04942
https://www.cnvd.org.cn/flaw/show/CNVD-2024-04941

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04945

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04944

4、Adobe 产品安全漏洞

Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-04927、CNVD-2024-04926、CNVD-2024-04930、CNVD-2024-04929、CNVD-2024-04928、CNVD-2024-04934、CNVD-2024-04933、CNVD-2024-04932）。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-2024-04927

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04926

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04930

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04929

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04928

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04934

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04933

https://www.cnvd.org.cn/flaw/show/CNVD-2024-04932

5、Tenda A18 缓冲区溢出漏洞

Tenda A18 是中国腾达（Tenda）公司的一款 AC1200 双频 Wi-Fi 中继器。本周，Tenda A18 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-2024-05739

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-2024-04954	D-Link DIR-619 formSetWAN_Wizard56 函数缓冲区溢出漏洞	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.dlink.com/
CNVD-2024-05287	Apple WebKit 代码执行漏洞	高	目前 Apple 已发布更新补丁，建议受影响用户升级至最新版本：

			https://www.apple.com.cn
CNVD-2024-05349	D-Link DIR-823G TXPower 参数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dlink.com/
CNVD-2024-05358	D-Link DIR-823G Type 参数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dlink.com/
CNVD-2024-05388	Google Android 权限提升漏洞（CNVD-2024-05388）	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/2023-10-01
CNVD-2024-05391	Google Android 代码执行漏洞（CNVD-2024-05391）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://android.googlesource.com/platform/frameworks/base/+/2d88a5c481df8986dbba2e02c5bf82f105b36243
CNVD-2024-05733	Tenda A15 deviceList 参数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-3187.html
CNVD-2024-05737	Tenda PA6 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.tenda.com.cn/download/detail-2986.html
CNVD-2024-06169	Huawei HarmonyOS 缓冲区溢出漏洞（CNVD-2024-06169）	高	厂商已提供漏洞修复方案，请关注厂商主页更新：https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202401-0000001799942565
CNVD-2024-06176	Hospital Management System 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://phpgurukul.com/hospital-management-system-in-php

小结：本周，D-Link 产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞导致拒绝服务。此外，Microsoft、Trend Micro、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞从堆内存中获取敏感信息，注入恶意脚本或 HTML 代码，提升权限，在系统上下文中执行任意代码等。另外，Tenda A18 被披露存在缓冲区溢出漏洞。攻击者可利用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、江西铭软科技有限公司 MCMS SQL 注入漏洞

验证描述

MCMS 是中国铭飞（MingSoft）公司的一个完整开源的 J2ee 系统。

江西铭软科技有限公司 MCMS v5.2.9 版本存在 SQL 注入漏洞，该漏洞源于/content/list.do 中的 categoryType 参数缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞获取数据库敏感数据。

验证信息

POC 链接：https://gitee.com/mingSoft/MCMS/issues/I8MAJK

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-06148

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. 思科产品曝出安全漏洞，允许黑客远程控制统一通信系统

该漏洞允许未经认证的远程威胁攻击者在受影响的设备上执行任意代码。

参考链接：https://www.freebuf.com/news/390855.html

2. Fortra 提醒客户注意新的 GoAnywhere 安全漏洞

Fortra 提醒客户注意 GoAnywhere MFT 新的身份验证绕过漏洞，该漏洞被跟踪为 CVE-2024-0204（CVSS 评分 9.8），一旦成功利用该漏洞，威胁攻击者就能够创建管理员用户。

参考链接：http://www.anquan419.com/knews/24/6581.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