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 15 日-2024 年 01 月 21 日 **2024 年第 3 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 488 个，其中高危漏洞 197 个、中危漏洞 261 个、低危漏洞 30 个。漏洞平均分值为 6.29。本周收录的漏洞中，涉及 0day 漏洞 348 个（占 71%），其中互联网上出现“WordPress 插件 WCFM Marketplace 跨站脚本漏洞、Hospital Management System 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漏洞总数 4975 个，与上周（4842 个）环比增加 3%。

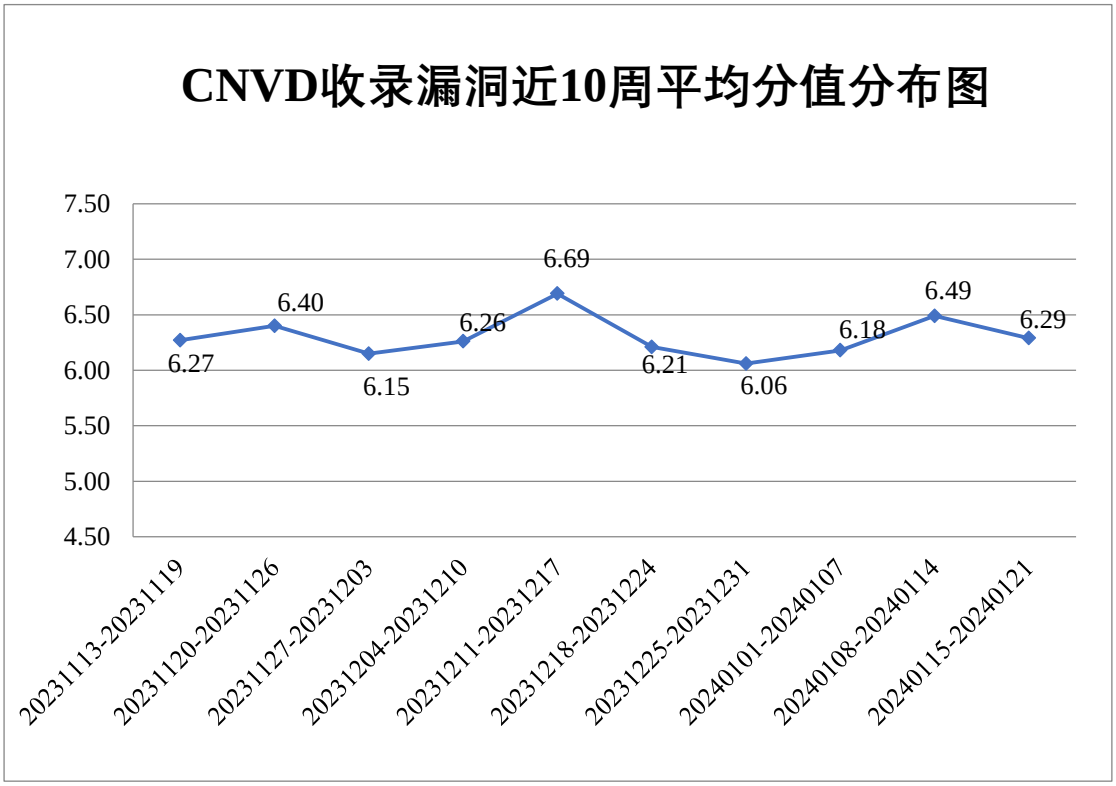

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 起，向基础电信企业通报漏洞事件 12 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 561 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 125 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 29 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：

珠海奔图电子有限公司、重庆金算盘软件有限公司、中山云易云软件科技有限公司、中环互联网、中广创思网络科技有限公司、智慧互通科技股份有限公司、正方软件股份有限公司、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、浙江大华技术股份有限公司、长沙市同迅计算机科技有限公司、云知声智能科技股份有限公司、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、熊猫智慧水务有限公司、兄弟（中国）商业有限公司、信呼、西门子（中国）有限公司、西安众邦网络科技有限公司、西安汇诚电信有限责任公司、武汉达梦数据库有限公司、卫宁健康科技集团股份有限公司、网宿科技股份有限公司、网是科技股份有限公司、万洲电气股份有限公司、万达宝软件（深圳）有限公司、天津荣联汇智智能科技有限公司、天津荣联汇智智慧科技有限公司、天地（常州）自动化股份有限公司、台达电子企业管理（上海）有限公司、苏州科达科技股份有限公司、四创科技有限公司、四川百信智创科技有限公司、世邦通信股份有限公司、施耐德电气（中国）有限公司、深圳智慧光迅信息技术有限公司、深圳市中电电力技术股份有限公司、深圳市星桐科技有限公司、深圳市鑫金浪电子有限公司、深圳市思迅软件股份有限公司、深圳市明源云科技有限公司、深圳市绿联科技股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市捷道智控实业有限公司、深圳市嘉荣华科技有限公司、深圳市吉祥腾达科技有限公司、深圳市福洽科技有限公司、深圳市道尔智控科技股份有限公司、深圳齐心好视通云计算有限公司、深圳古瑞瓦特新能源有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海盈策信息技术有限公司、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、上海嘉扬信息系统有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、上海海典软件股份有限公司、上海泛微网络科技股份有限公司、上海必智科技有限公司、上海宝信软件股份有限公司、上海安达通信息安全技术股份有限公司、上海艾泰科技有限公司、商派软件有限公司、善理通益信息科技有限公司、山东运筹软件有限公司、山东云时空信息科技有限公司、山东科德电子有限公司、山东金钟科技集团股份有限公司、山东比特智能科技股份有限公司、厦门物之联智能科技有限公司、厦门快普信息技术有限公司、厦门海为科技有限公司、三星（中国）投资有限公司、青岛海威茨仪表有限公司、桥西区雪洛软件开发工作室、普联技术有限公司、南宁迈世信

息技术有限公司、南宁比优网络科技有限公司、南京纳龙科技有限公司、南京东大智能化系统有限公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、辽宁苍腾华夏卡友网络服务有限公司、联奕科技股份有限公司、联想图像（北京）科技有限公司、蓝网科技股份有限公司、京师博仁（北京）科技发展股份公司、劲旅环境科技股份有限公司、江苏天瑞仪器股份有限公司、江苏金智教育信息股份有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、华讯高科股份有限公司、河南航飞光电科技有限公司、杭州易软共创网络科技有限公司、杭州伊柯夫科技有限公司、杭州雄伟科技开发股份有限公司、杭州瀚洋科技有限公司、海尔集团电子商务有限公司、广州优胜特软件开发有限公司、广州盈可视电子科技有限公司、广州市和丰自动化科技有限公司、广州市保伦电子有限公司、广联达科技股份有限公司、广东飞企互联科技股份有限公司、广东堡塔安全技术有限公司、广东保伦电子股份有限公司、东华医为科技有限公司、东莞哲霖信息科技有限公司、鼎捷软件股份有限公司、大唐电信科技股份有限公司、成都虚谷伟业科技有限公司、成都睿联未来科技有限公司、成都飞鱼星科技股份有限公司、超威半导体产品（中国）有限公司、畅捷通信息技术股份有限公司、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、北京星网锐捷网络技术有限公司、北京天融信网络安全技术有限公司、北京数字政通科技股份有限公司、北京巧巧时代网络科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京华宇信息技术有限公司、北京宏景世纪软件股份有限公司、北京国炬信息技术有限公司、北京广慧金通教育科技有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、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、安徽皖通邮电股份有限公司、阿里巴巴集团安全应急响应中心、ZZCMS、zbzcms 和 Lexmark。

本周，CNVD 发布了《Oracle 发布 2024 年 1 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9661

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、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、北京数字观星科技有限公司、新华三技术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、北京卓识网安技术股份有限公司、贵州多彩网安科技有限公司、内蒙古洞明科技有限公司、联想集团、快页信息技术有限公司、安徽锋刃信息科技有限公司、河南东方云盾信息技术有限公司、亚信科技（成都）有限公司、北京山石网科信息技术有限公司、安全邦（北京）信息技术有限公司、杭州默安科技有限公司、江苏晟晖信息科技有限公司、上海观安信息技术股份有限公司、中国电信股份有限公司上海研究院、江苏云天网络安全技术

有限公司、奇安星城网络安全运营服务（长沙）有限公司、江苏天竞云合数据技术有限公司、任子行网络技术股份有限公司、博智安全科技股份有限公司、中粤网安技术（广东）有限公司、湖北星野科技发展有限公司、中孚安全技术有限公司、南京先维信息技术有限公司、上海直画科技有限公司、杭州安信检测技术有限公司、福建福诺移动通信技术有限公司、苏州棱镜七彩信息科技有限公司、北京君云天下科技有限公司、建信金科网络攻击实验室、赛尔网络有限公司、软通动力信息技术（集团）股份有限公司、北京中关村实验室、西藏熙安信息技术有限责任公司、中国国际工程咨询有限公司、浙江工业大学、中华人民共和国上海海事局、上海齐同信息科技有限公司、江苏百达智慧网络科技有限公司（含光实验室）、TISEC 洪椒战队、信息产业信息安全测评中心、北京网御星云信息技术有限公司、北京天防安全科技有限公司、济南三泽信息安全测评有限公司、河南悦海数安科技有限公司、杭州美创科技有限公司、江苏极元信息技术有限公司、中国科学院信息工程研究所、西安秦易信息技术有限公司、北京科技大学、杭州智顺科技有限公司、瑞数信息技术（上海）有限公司及其他个人白帽子向 CNVD 提交了 4975 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）、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 3147 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
奇安信网神（补天平台）	1205	1205
北京神州绿盟科技有限公司	707	0
斗象科技（漏洞盒子）	705	705
三六零数字安全科技集团有限公司	640	640
上海交大	597	597
北京启明星辰信息安全技术有限公司	595	9
深信服科技股份有限公司	483	0
北京数字观星科技有限公司	386	0
新华三技术有限公司	309	0
杭州安恒信息技术股份有限公司	302	253

安天科技集团股份有限公司	240	0
中国电信集团系统集成有限责任公司	152	0
北京知道创宇信息技术有限公司	89	0
北京安信天行科技有限公司	29	29
北京天融信网络安全技术有限公司	15	15
杭州迪普科技股份有限公司	10	0
阿里云计算有限公司	5	5
北京智游网安科技有限公司	3	3
西安四叶草信息技术有限公司	2	2
内蒙古奥创科技有限公司	1	1
江苏金盾检测技术股份有限公司	125	125
北京卓识网安技术股份有限公司	91	91
贵州多彩网安科技有限公司	65	65
内蒙古洞明科技有限公司	47	47
联想集团	42	42
快页信息技术有限公司	37	37
安徽锋刃信息科技有限公司	29	29
河南东方云盾信息技术有限公司	27	27
亚信科技（成都）有	18	18

限公司		
北京山石网科信息技术有限公司	11	11
安全邦（北京）信息技术有限公司	9	9
杭州默安科技有限公司	8	8
江苏晟晖信息科技有限公司	7	7
上海观安信息技术股份有限公司	6	6
中国电信股份有限公司上海研究院	6	6
江苏云天网络安全技术有限公司	6	6
奇安星城网络安全运营服务（长沙）有限公司	5	5
江苏天竞云合数据技术有限公司	5	5
任子行网络技术股份有限公司	3	3
博智安全科技股份有限公司	3	3
中粤网安技术（广东）有限公司	2	2
湖北星野科技发展有限公司	2	2
中孚安全技术有限公司	2	2
南京先维信息技术有限公司	2	2
上海直画科技有限公司	2	2
杭州安信检测技术有	2	2

限公司		
福建福诺移动通信技术有限公司	2	2
苏州棱镜七彩信息科技有限公司	2	2
北京君云天下科技有限公司	1	1
建信金科网络攻击实验室	1	1
赛尔网络有限公司	1	1
软通动力信息技术（集团）股份有限公司	1	1
北京中关村实验室	1	1
西藏熙安信息技术有限责任公司	1	1
中国国际工程咨询有限公司	1	1
浙江工业大学	1	1
中华人民共和国上海海事局	1	1
上海齐同信息科技有限公司	1	1
江苏百达智慧网络科技有限公司（含光实验室）	1	1
TISEC 洪椒战队	1	1
信息产业信息安全测评中心	1	1
北京网御星云信息技术有限公司	1	1
北京天防安全科技有限公司	1	1
济南三泽信息安全测评有限公司	1	1

河南悦海数安科技有限公司	1	1
杭州美创科技有限公司	1	1
江苏极元信息技术有限公司	1	1
中国科学院信息工程研究所	1	1
西安秦易信息技术有限公司	1	1
北京科技大学	1	1
杭州智顺科技有限公司	1	1
瑞数信息技术（上海）有限公司	1	1
CNCERT 广西分中心	7	7
CNCERT 陕西分中心	1	1
个人	913	913
报送总计	7986	4975

本周漏洞按类型和厂商统计

本周，CNVD 收录了 488 个漏洞。WEB 应用 187 个，应用程序 169 个，网络设备（交换机、路由器等网络端设备）77 个，操作系统 21 个，智能设备（物联网终端设备）20 个，安全产品 11 个，数据库 2 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	187
应用程序	169
网络设备（交换机、路由器等网络端设备）	77
操作系统	21
智能设备（物联网终端设备）	20
安全产品	11
数据库	2
车联网	1

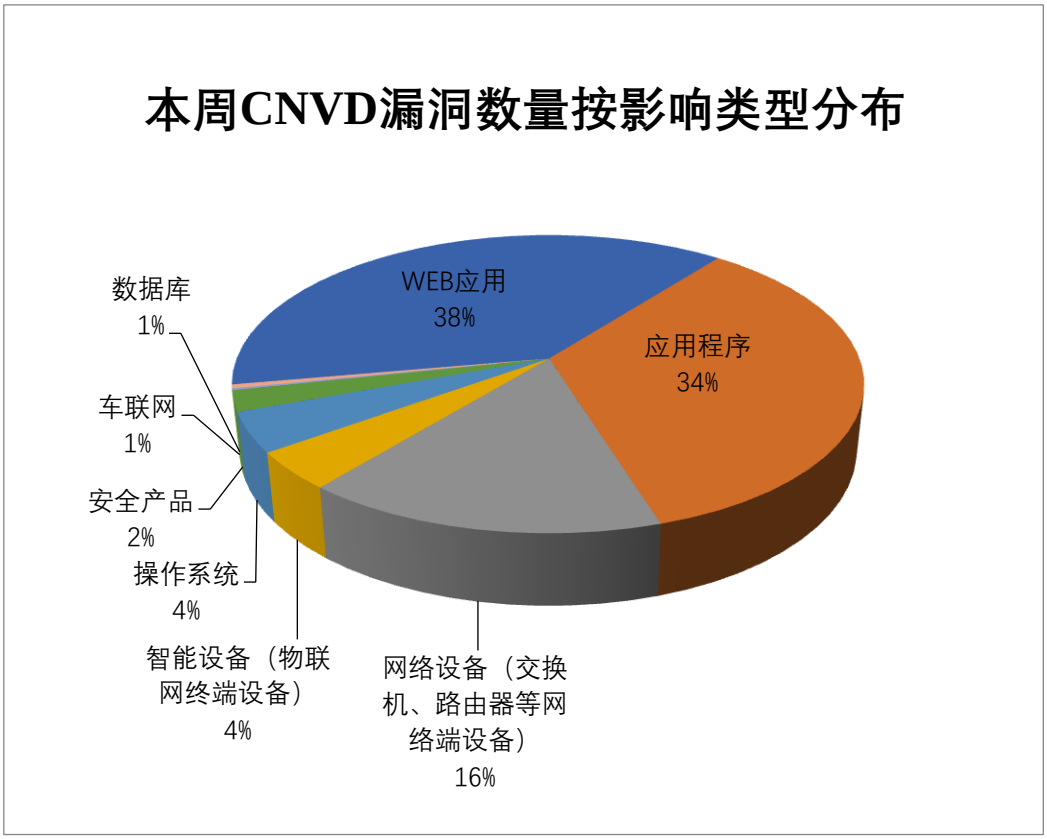

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、GTKWave、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	Adobe	45	9%
2	GTKWave	20	4%
3	Google	16	3%
4	TOTOLINK	16	3%
5	北京星网锐捷网络技术有限公司	15	3%
6	Microsoft	12	3%
7	北京百卓网络技术有限公司	12	3%
8	用友网络科技股份有限公司	12	3%
9	Tenda	11	2%
10	其他	329	67%

本周行业漏洞收录情况

本周，CNVD 收录了 49 个电信行业漏洞，40 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Tenda AX1803 缓冲区溢出漏洞、Google Android 信

息泄露漏洞（CNVD-2024-02704）”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/

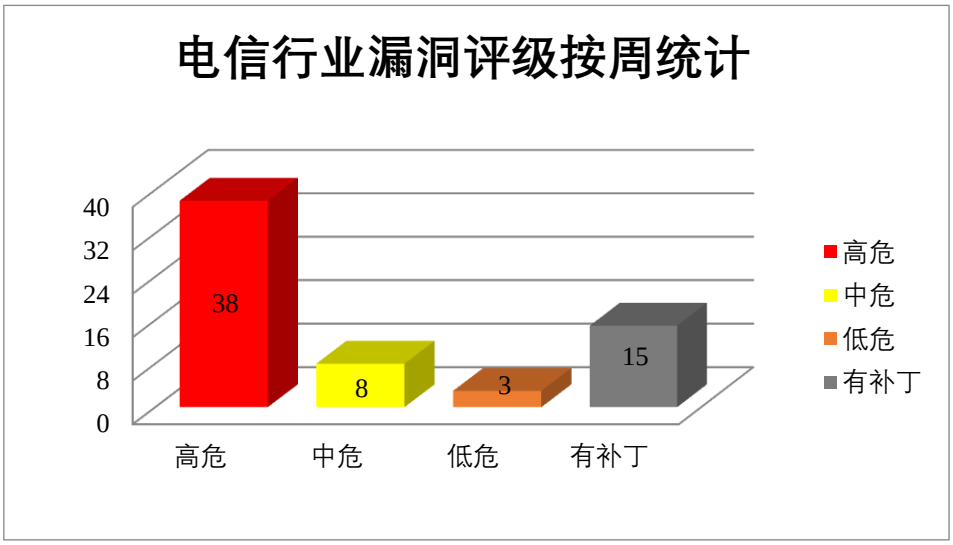

图 3 电信行业漏洞统计

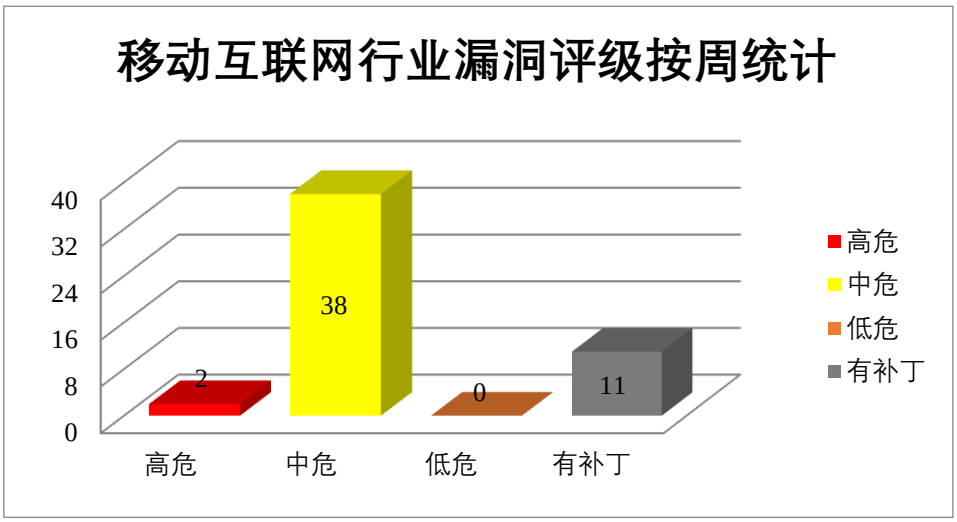

图 4 移动互联网行业漏洞统计

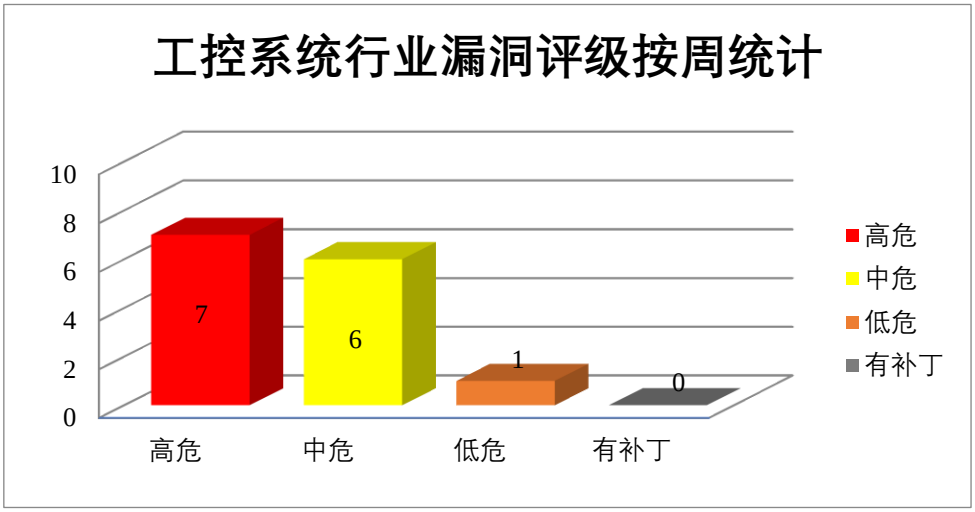

图 5 工控系统行业漏洞统计

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、 Tenda 产品安全漏洞

Tenda AX1803 是中国腾达（Tenda）公司的一款双频千兆 WIFI6 路由器。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞在系统上执行任意代码或者导致拒绝服务。

CNVD 收录的相关漏洞包括：Tenda AX1803 缓冲区溢出漏洞（CNVD-2024-02208、CNVD-2024-02211、CNVD-2024-02210、CNVD-2024-02209、CNVD-2024-02214、CNVD-2024-02213、CNVD-2024-02212、CNVD-2024-02217）。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-2024-02208

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02211

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02210

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02209

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02214

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02213

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02212

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02217

2、 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。Adobe RoboHelp Server 是面向 FrameMaker 和 RoboHelp 企业用户的基于服务器的应用

程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞查看、添加、修改或删除后端数据库中的信息，系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Substance 3D Stager 越界读取漏洞（CNVD-2024-02723、CNVD-2024-02724、CNVD-2024-02725、CNVD-2024-02726、CNVD-2024-02727）、Adobe RoboHelp Server SQL 注入漏洞、Adobe RoboHelp Server 信息泄露漏洞、Adobe RoboHelp Server 路径遍历漏洞。其中，“Adobe RoboHelp Server 信息泄露漏洞、Adobe RoboHelp Server 路径遍历漏洞”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-2024-02723
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02724
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02725
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02726
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02727
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02728
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02729
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02730

3、 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，攻击者可利用漏洞获取敏感信息，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-2024-02335）、Google Android 代码执行漏洞（CNVD-2024-02336、CNVD-2024-02677）、Google Android 信息泄露漏洞（CNVD-2024-02678、CNVD-2024-02704、CNVD-2024-02705、CNVD-2024-02706、CNVD-2024-02707）。其中，“Google Android 权限提升漏洞（CNVD-2024-02335）、Google Android 代码执行漏洞（CNVD-2024-02336、CNVD-2024-02677）、Google Android 信息泄露漏洞（CNVD-2024-02704）”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-2024-02335
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02336
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02677
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02678
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02704
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02705

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02706

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02707

4、 Microsoft 产品安全漏洞

Microsoft .NET 是一个致力于敏捷软件开发、快速应用开发、平台无关性和网络透明化的软件框架。Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Office 是美国微软（Microsoft）公司的一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。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限制，获取 SYSTEM 权限，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft .NET 拒绝服务漏洞（CNVD-2024-02713）、Microsoft Excel 执行代码漏洞、Microsoft Excel 安全功能绕过漏洞（CNVD-2024-02715）、Microsoft Office 执行代码漏洞（CNVD-2024-02716、CNVD-2024-02722）、Microsoft Office 安全功能绕过漏洞（CNVD-2024-02717、CNVD-2024-02720）、Microsoft Office 权限提升漏洞（CNVD-2024-02721）。其中，除“Microsoft Office 安全功能绕过漏洞（CNVD-2024-02720）”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-2024-02713

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02714

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02715

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02716

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02717

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02720

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02721

https://www.cnvd.org.cn/flaw/show/CNVD-2024-02722

5、TRENDnet TV-IP1314PI 缓冲区溢出漏洞

TRENDnet TV-IP1314PI 是美国趋势网络（TRENDnet）公司的一款无线网络摄像机。本周，TRENDnet TV-IP1314PI 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞导致任意命令执行。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-2024-02732

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-2024-02206	IBM DB2 权限提升漏洞（CNVD-2024-02206）	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/7105500
CNVD-2024-02218	Tenda AX1803 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-3421.html
CNVD-2024-02960	Emlog SQL 注入漏洞（CNVD-2024-02960）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/emlog/emlog/issues/144
CNVD-2024-02959	LibreOffice 加密问题漏洞（CNVD-2024-02959）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.libreoffice.org/about-us/security/advisories/cve-2022-26307
CNVD-2024-04848	GTKWave 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gtkwave.sourceforge.net/
CNVD-2024-04850	GTKWave 任意写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gtkwave.sourceforge.net/
CNVD-2024-04887	FreeImage ReadPalette 方法拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/freeimage/bugs/334/
CNVD-2024-04886	FreeImage ReadImageLine 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/freeimage/discussion/36111/thread/afb98701eb/
CNVD-2024-04914	TOTOLINK EX1200T 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/148/ids/36.html
CNVD-2024-04921	TOTOLINK N350RT password 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.totolink.net/home/menu/detail/menu_listtpl/download/id/206/ids/36.html

小结：本周，Tenda 产品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。此外，Adobe、Google、Microsoft 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限制，获取敏感信息，提升权限，在系统上

执行任意代码等。另外，TRENDnet TV-IP1314PI 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞导致任意命令执行。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、WordPress 插件 WCFM Marketplace 跨站脚本漏洞

验证描述

WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

WordPress 插件 WCFM Marketplace 存在跨站脚本漏洞，该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://plugins.trac.wordpress.org/browser/wc-multivendor-marketplace/tags/3.6.1/views/store-lists/wcfmmp-view-store-lists.php#L207

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-02731

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. Ivanti Connect Secure 曝两个安全漏洞，已被大规模利用

威胁情报公司 Volexity 发现，影响 Ivanti 的 Connect Secure VPN 和 Policy Secure 网络访问控制（NAC）设备的两个零日漏洞正在被大规模利用。自 1 月 11 日开始，多个威胁组织在大范围攻击中利用 CVE-2023-46805 身份验证绕过和 CVE-2024-21887 命令注入漏洞。

参考链接：https://www.bleepingcomputer.com/news/security/ivanti-connect-secure-zero-days-now-under-mass-exploitation/

2. 可绕过邮件验证劫持账号，GitLab 紧急修复 CVSS 满分密码重置漏洞

GitLab 日前为社区版（CE）及企业版（EE）推出 16.7.2、16.6.4 及 16.5.6 安全更

新，重点修复了 CVSS 风险评分达到 10 分的密码重置漏洞 CVE-2023-7028。

参考链接：https://www.ithome.com/0/745/480.htm

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