国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 06 月 24 日-2024 年 06 月 30 日 **2024 年第 26 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 175 个、中危漏洞 222 个、低危漏洞 9 个。漏洞平均分值为 6.42。本周收录的漏洞中，涉及 0day 漏洞 297 个（占 73 %），其中互联网上出现“TP-Link TL-7DR5130 安全绕过漏洞、Tenda FH1206 命令执行漏洞”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 16683 个，与上周（14284 个）环比增加 17%。

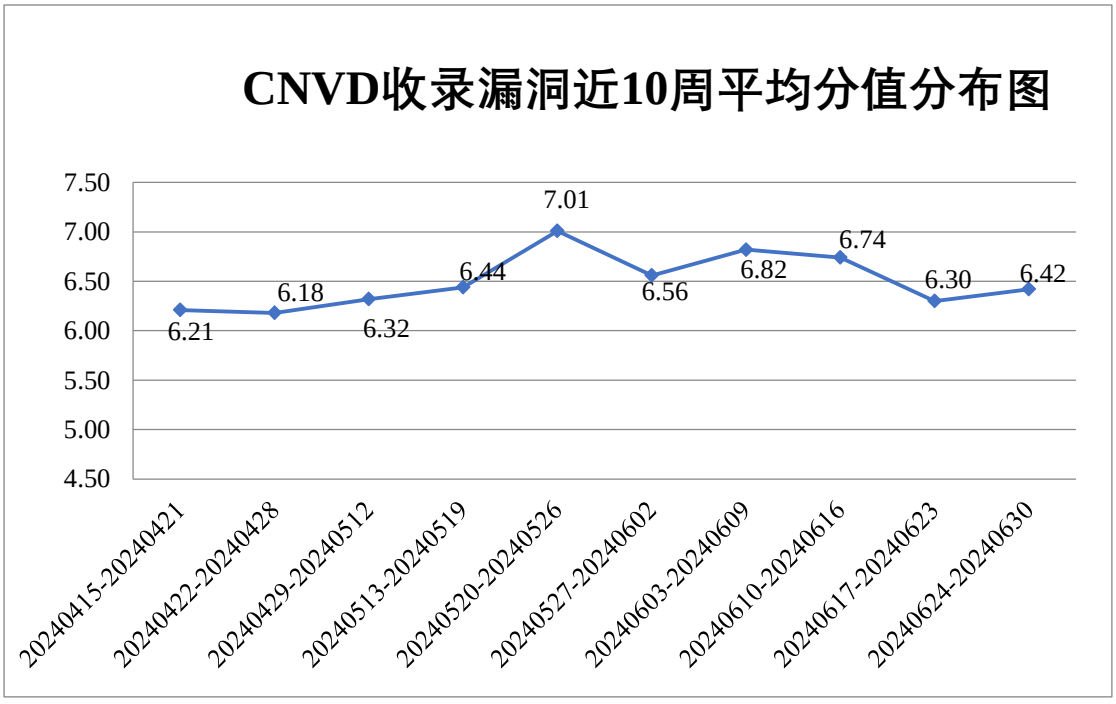

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 11 起，向基础电

信企业通报漏洞事件 6 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 699 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 80 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 15 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：

紫光软件系统有限公司、众勤通信设备贸易（上海）有限公司、中科方德软件有限公司、中电信量子科技有限公司、智互联（深圳）科技有限公司、浙江和达科技股份有限公司、浙江好络维医疗技术有限公司、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、新天科技股份有限公司、小米科技有限责任公司、襄阳软宝信息科技有限公司、西安众邦网络科技有限公司、武汉金同方科技有限公司、武汉合智数字能源技术有限公司、温州市易天信息科技有限公司、卫宁健康科技集团股份有限公司、网件（北京）网络技术有限公司、万洲电气股份有限公司、统信软件技术有限公司、腾讯安全应急响应中心、速达软件技术（广州）有限公司、苏州骏驰网络科技有限公司、施耐德电气（中国）有限公司、深圳维盟网络技术有限公司、深圳拓安信物联股份有限公司、深圳市中电数通智慧安全科技股份有限公司、深圳市有为信息技术发展有限公司、深圳市明源云科技有限公司、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、深圳市宏电技术股份有限公司、深圳市国信合成科技有限公司、深圳市道尔智控科技股份有限公司、深圳市爱施德股份有限公司、深圳前海华夏智信数据科技有限公司、深圳开维信息技术股份有限公司、深圳华视美达信息技术有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海真兰仪表科技股份有限公司、上海桑锐电子科技股份有限公司、上海九翊软件科技有限公司、上海华测导航技术股份有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海发那科机器人有限公司、上海顶想信息科技有限公司、上海博达数据通信有限公司、上海艾泰科技有限公司、商派软件有限公司、山东科大中天安控科技有限公司、山东聚恒网络技术有限公司、厦门亿联网络技术股份有限公司、厦门四信通信科技有限公司、厦门科拓通讯技术股份有限公司、三菱电机株式会社、任子行网络技术股份有限公司、青岛东胜伟业软件有限公司、青岛爱米云软件有限公司、麒麟软件有限公司、鹏为软件股份有限公司、南京星远图科技有限公司、南昌航天广信科技有限责任公司、龙采科技集团有限责任公司、力合科技（湖南）股份有限公司、廊坊市极致网络科技有限公司、江苏天捷信息技术有限公司、江苏赛达电子科技有限公司、江苏麦维智能科技有限公司、济南瑞泉电子有限公司、吉翁电子（深圳）有限公司、吉林省慧海科技信息有限公司、恒信汽车集团股份有限公司、杭州新中大科技股份有限公司、杭州荷花软件有限公司、杭州海康威视数字技术股份有限公司、广州市保伦电子有限公司、广州赛意信息科技股份有限公司、广州热点软件科技股份有限公司、广州好象科技有限公司、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、东莞市宇腾信息科技有限公司、东北师大理想软件股份有限公司、成都科鸿智信科技有限公司、畅捷通信息技术股份有限公司、北京中控科技发展有限公司、北京中科商软软件有限公司、北京中创视讯科技有限公司、北京智齿博创科技有限公司、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、北京万户软件技术有限公司、北京数字政通科技股份有限公司、北京神州视翰科技有限公司、北京神州绿盟科技有限公司、北京人大金仓信息技术股份有限公司、北京平凯星辰科技发展有限公司、北京谋智火狐信息技术有限公司、北京美特软件技术有限公司、北京旷视科技有限公司、北京金和网络股份有限公司、北京国炬信息技术有限公司、北京超图软件股份有限公司、北京百卓网络技术有限公司、北京奥特美克科技股份有限公司、北京爱科农科技有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、爱瑞思软件（深圳）有限公司、阿里巴巴集团安全应急响应中心和 YeaLink。

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、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等单位报送公开收集的漏洞数量较多。河南东方云盾信息技术有限公司、江苏金盾检测技术股份有限公司、快页信息技术有限公司、成都久信信息技术股份有限公司、北京远禾科技有限公司、北京翰慧投资咨询有限公司、重庆都会信息科技有限公司、中国电信股份有限公司上海研究院、江苏极元信息技术有限公司、中孚安全技术有限公司、江西中和证信息安全技术有限公司、马鞍山书拓安全科技有限公司、江苏云天网络安全技术有限公司、安徽天行网安信息安全技术有限公司、人保信息科技有限公司、苏州棱镜七彩信息科技有限公司、河南宝通信息安全测评有限公司、国网江西省电力有限公司电力科学研究院、北京天防安全科技有限公司、黄河勘测规划设计研究院有限公司、深圳昂楷科技有限公司、上海只柏特信息技术有限公司、河南灵创电子科技有限公司、成都愚安科技有限公司、成都思维世纪科技有限责任公司、成都安美勤信息技术股份有限公司、湖南省电子信息产业研究院、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、国网宁夏电力有限公司石嘴山供电公司、海南神州希望网络有限公司、四川电科宏安科技有限公司、河南天祺信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 16683 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 15326 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）	9973	9973
斗象科技（漏洞盒子）	3790	3790
北京神州绿盟科技有限公司	1487	0
三六零数字安全科技集团有限公司	1270	1270
北京启明星辰信息安全技术有限公司	875	0
新华三技术有限公司	816	0
安天科技集团股份有限公司	446	0
北京天融信网络安全技术有限公司	367	14
阿里云计算有限公司	324	0
上海交大	293	293
北京数字观星科技有限公司	279	0
远江盛邦（北京）网络安全科技股份有限公司	197	197
华为技术有限公司	92	0
北京长亭科技有限公司	61	0
恒安嘉新（北京）科技股份公司	60	0
中国电信股份有限公司网络安全产品运营中心	44	44
北京知道创宇信息技术有限公司	44	0
京东科技信息技术有限公司	22	0
北京升鑫网络科技有限公司（青藤云）	17	17

杭州迪普科技股份有限公司	12	2
北京智游网安科技有限公司	4	4
杭州安恒信息技术股份有限公司	1	0
河南东方云盾信息技术有限公司	47	47
江苏金盾检测技术股份有限公司	32	32
快页信息技术有限公司	22	22
成都久信信息技术股份有限公司	16	16
北京远禾科技有限公司	9	9
北京翰慧投资咨询有限公司	8	8
重庆都会信息科技有限公司	7	7
中国电信股份有限公司上海研究院	7	7
江苏极元信息技术有限公司	5	5
中孚安全技术有限公司	5	5
江西中和证信息安全技术有限公司	4	4
马鞍山书拓安全科技有限公司	3	3
江苏云天网络安全技术有限公司	3	3
安徽天行网安信息安全技术有限公司	3	3
人保信息科技有限公	2	2

司		
苏州棱镜七彩信息科技有限公司	2	2
河南宝通信息安全测评有限公司	2	2
国网江西省电力有限公司电力科学研究院	2	2
北京天防安全科技有限公司	2	2
黄河勘测规划设计研究院有限公司	2	2
深圳昂楷科技有限公司	2	2
上海只柏特信息技术有限公司	1	1
河南灵创电子科技有限公司	1	1
成都愚安科技有限公司	1	1
成都思维世纪科技有限责任公司	1	1
成都安美勤信息技术股份有限公司	1	1
湖南省电子信息产业研究院	1	1
中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）	1	1
国网宁夏电力有限公司石嘴山供电公司	1	1
海南神州希望网络有限公司	1	1
四川电科宏安科技有限公司	1	1

河南天祺信息安全技术有限公司	1	1
CNCERT 内蒙古分中心	3	3
CNCERT 宁夏分中心	1	1
个人	879	879
报送总计	21553	16683

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 195 个，应用程序 155 个，网络设备（交换机、路由器等网络端设备）29 个，操作系统 11 个，智能设备（物联网终端设备）11 个，安全产品 3 个，数据库 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	195
应用程序	155
网络设备（交换机、路由器等网络端设备）	29
操作系统	11
智能设备（物联网终端设备）	11
安全产品	3
数据库	2

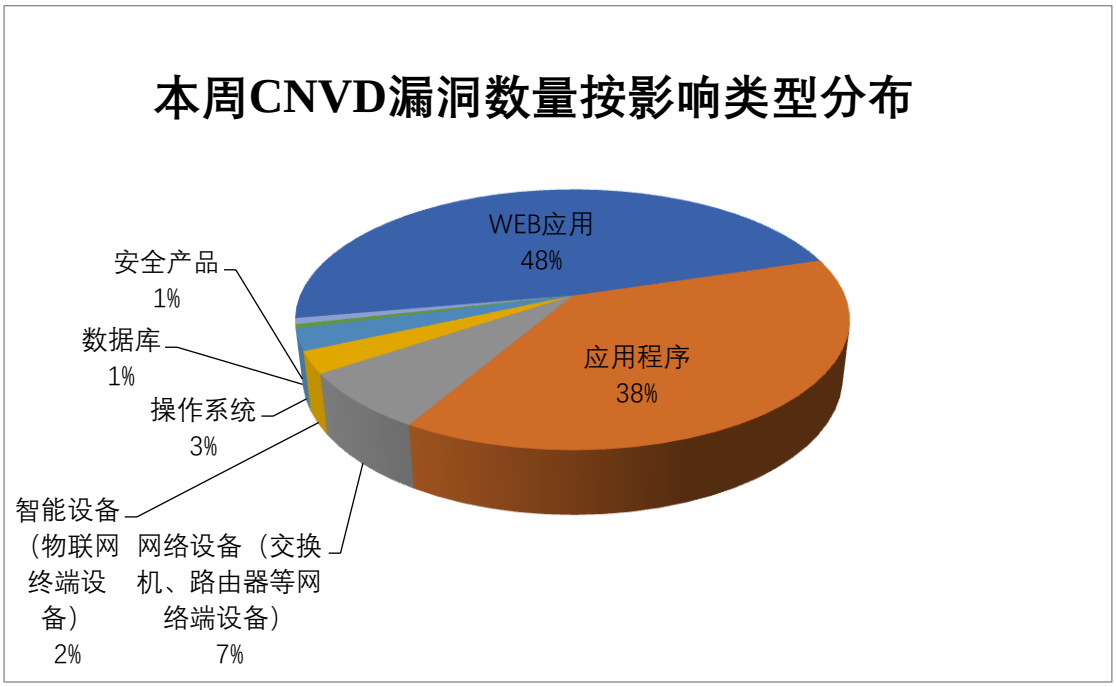

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、Microsoft 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	50	12%
2	Adobe	30	7%
3	Microsoft	17	4%
4	OneFlo	12	3%
5	Mozilla	12	3%
6	Dell	10	3%
7	厦门科拓通讯技术股份有限公司	8	2%
8	ros-navigation	8	2%
9	福建科立讯通信有限公司	6	2%
10	其他	253	62%

本周行业漏洞收录情况

本周，CNVD 收录了 20 个电信行业漏洞，15 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2024-29663）、Delta Electronics DIAEnergie 授权问题漏洞（CNVD-2024-29664）”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/

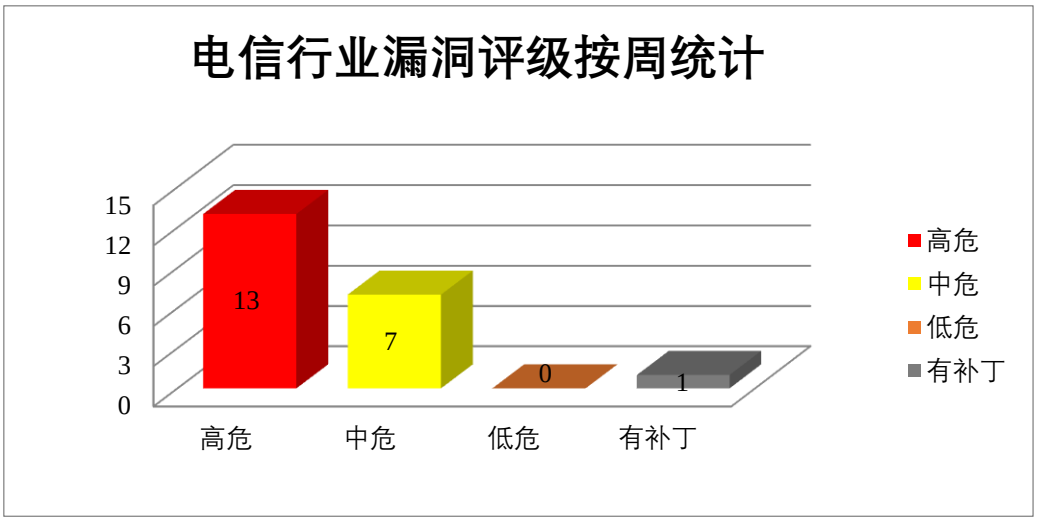

图 3 电信行业漏洞统计

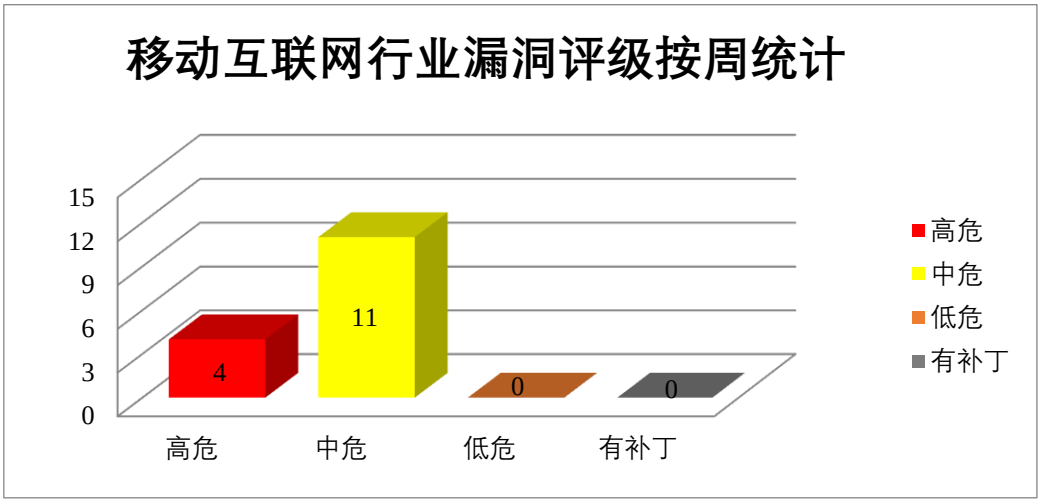

图 4 移动互联网行业漏洞统计

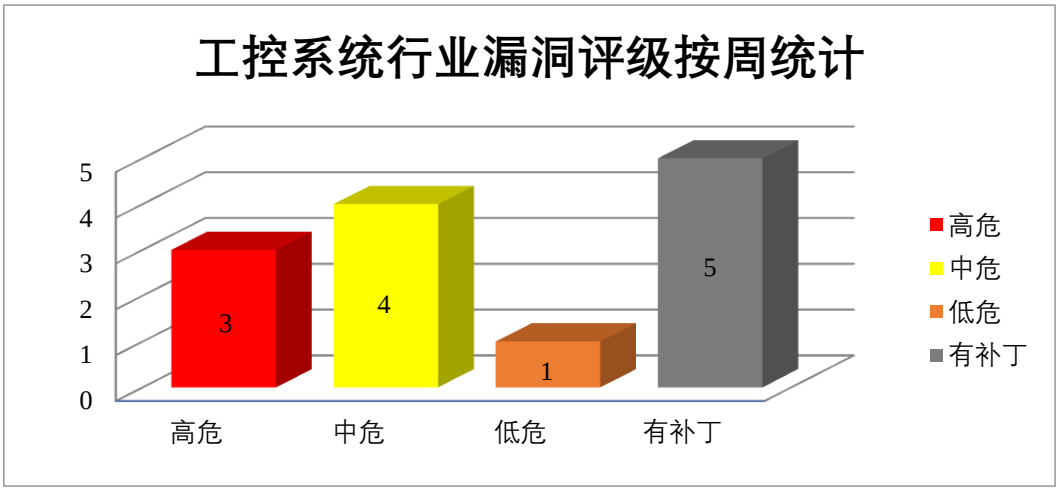

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

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，攻击者可利用漏洞绕过安全限制，通过精心制作的 HTML 页面从进程内存中获取潜在的敏感信息，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2024-29279、CNVD-2024-29277、CNVD-2024-29281、CNVD-2024-29286、CNVD-2024-29285）、Google Chrome 代码执行漏洞（CNVD-2024-29284、CNVD-2024-29287）、Google Chrome 越界读取漏洞（CNVD-2024-29282）。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-2024-29279

https://www.cnvd.org.cn/flaw/show/CNVD-2024-29277
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29284
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29282
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29281
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29287
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29286
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29285

2、 Microsoft 产品安全漏洞

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。Microsoft SharePoint Server 是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 Outlook 是一套电子邮件应用程序。Microsoft Exchange Server 是一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，在系统上执行任意代码，获取 SYSTEM 权限等。

CNVD 收录的相关漏洞包括：Microsoft Office 远程代码执行漏洞（CNVD-2024-28624、CNVD-2024-28698、CNVD-2024-28697）、Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2024-28700）、Microsoft Outlook 远程代码执行漏洞（CNVD-2024-28699）、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2024-28704）、Microsoft Outlook for Windows 欺骗漏洞、Microsoft Office 权限提升漏洞（CNVD-2024-28705）。其中，除“Microsoft Office 远程代码执行漏洞（CNVD-2024-28698）、Microsoft Office 权限提升漏洞（CNVD-2024-28705）”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-2024-28624
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28698
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28697
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28700
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28699
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28704
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28703
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28705

3、 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。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，破坏堆栈并导致浏览器崩溃在系

统上执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 安全绕过漏洞（CNVD-2024-29140、CNVD-2024-29138、CNVD-2024-29141、CNVD-2024-29334）、Mozilla Firefox 释放后重用漏洞（CNVD-2024-29142、CNVD-2024-29144）、Mozilla Firefox 信息泄露漏洞（CNVD-2024-29332）、Mozilla Firefox 内存损坏漏洞（CNVD-2024-29331）。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-2024-29140
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29138
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29142
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29141
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29144
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29332
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29331
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29334

4、 Adobe 产品安全漏洞

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措施并获取未经授权的访问，导致任意代码执行等。

CNVD 收录的相关漏洞包括：Adobe Commerce 身份验证错误漏洞、Adobe Commerce 授权问题漏洞（CNVD-2024-28954）、Adobe Commerce XML 外部实体注入漏洞、Adobe Commerce 输入验证错误漏洞（CNVD-2024-28959、CNVD-2024-28958）、Adobe Commerce 服务器端请求伪造漏洞、Adobe Commerce 文件上传漏洞、Adobe Commerce 命令注入漏洞。上述 8 个漏洞的综合评级为“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-2024-28952
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28954
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28953
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28959
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28958
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28961
https://www.cnvd.org.cn/flaw/show/CNVD-2024-28960
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29338

5、D-Link DIR-605L 硬编码密码漏洞

D-Link DIR-605L 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-605L 被披露存在硬编码密码漏洞。攻击者可利用该漏洞以 root 身份登录并获取管理员权限。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-2024-29649

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-2024-28708	FFmpeg 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/FFmpeg/FFmpeg/commit/d2e8974699a9e35cc1a926bf74a972300d629cd5
CNVD-2024-28709	FFmpeg 命令执行漏洞（CNVD-2024-28709）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/FFmpeg/FFmpeg/commit/ca09d8a0dcd82e3128e62463231296aaf63ae6f7
CNVD-2024-29137	Mozilla Firefox 欺骗漏洞（CNVD-2024-29137）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2024-27/
CNVD-2024-29143	Mozilla Firefox 内存安全漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/security/advisories/mfsa2024-25/
CNVD-2024-29278	Google Chrome 数据验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_16.html
CNVD-2024-29336	Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2024-29336）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb24-07.html
CNVD-2024-29333	Mozilla Firefox 释放后重用漏洞（CNVD-2024-29333）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/security/advisories/mfsa2024-25/

CNVD-2024-29339	Adobe ColdFusion 安全绕过漏洞（CNVD-2024-29339）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://helpx.adobe.com/security/products/coldfusion/apsb23-47.html
CNVD-2024-29344	Dell Common Event Enabler 反序列化漏洞	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.dell.com/support/kbdoc/en-us/000224987/dsa-2024-179-security-update-for-dell-emc-common-event-enabler-windows-for-cavatools-vulnerabilities
CNVD-2024-29349	Fortinet FortiWeb 操作系统命令注入漏洞（CNVD-2024-29349）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-22-131

小结：本周，Google 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，通过精心制作的 HTML 页面从进程内存中获取潜在的敏感信息，在系统上执行任意代码等。此外，Microsoft、Mozilla、Adobe 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措施并获取未经授权的访问，破坏堆栈并导致浏览器崩溃在系统上执行任意代码等。另外，D-Link DIR-605L 被披露存在硬编码密码漏洞。攻击者可利用漏洞以 root 身份登录并获取管理员权限。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、Tenda FH1206 命令执行漏洞

验证描述

Tenda FH1206 是中国腾达（Tenda）公司的一款无线路由器。

Tenda FH1206 1.2.0.8(8155)版本存在命令执行漏洞，该漏洞源于 ip/goform/formexeCommand 的 cmdinput 参数未能正确过滤构造命令特殊字符、命令等，攻击者可利用该漏洞在系统上执行任意命令。

验证信息

POC 链接：https://palm-vertebra-fe9.notion.site/formexeCommand_RCE-91a5f12ae23a42b4a25f5d1d4de308da

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-29652

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. GitLab 曝一安全漏洞，威胁软件开发管道

该公司正敦促运行易受攻击版本的用户立即修补该漏洞，以避免 CI/CD 失常。

参考链接：https://www.freebuf.com/news/404873.html

2. 5G 连接存在漏洞，移动设备易被绕过或受到 DoS 攻击

宾夕法尼亚州立大学的研究人员已经向各自的移动供应商报告了他们发现的所有漏洞，这些供应商都已经部署了补丁。

参考链接：https://www.freebuf.com/news/404737.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