国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 07 月 22 日-2024 年 07 月 28 日 **2024 年第 30 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 223 个，其中高危漏洞 151 个、中危漏洞 37 个、低危漏洞 35 个。漏洞平均分值为 6.69。本周收录的漏洞中，涉及 0day 漏洞 19 个（占 9%），其中互联网上出现“Farm Management System SQL 注入漏洞（CNVD-2024-33389）、 Opencart 跨站请求伪造漏洞（CNVD-2024-33388）”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 54241 个，与上周（14074）环比增加 285%。

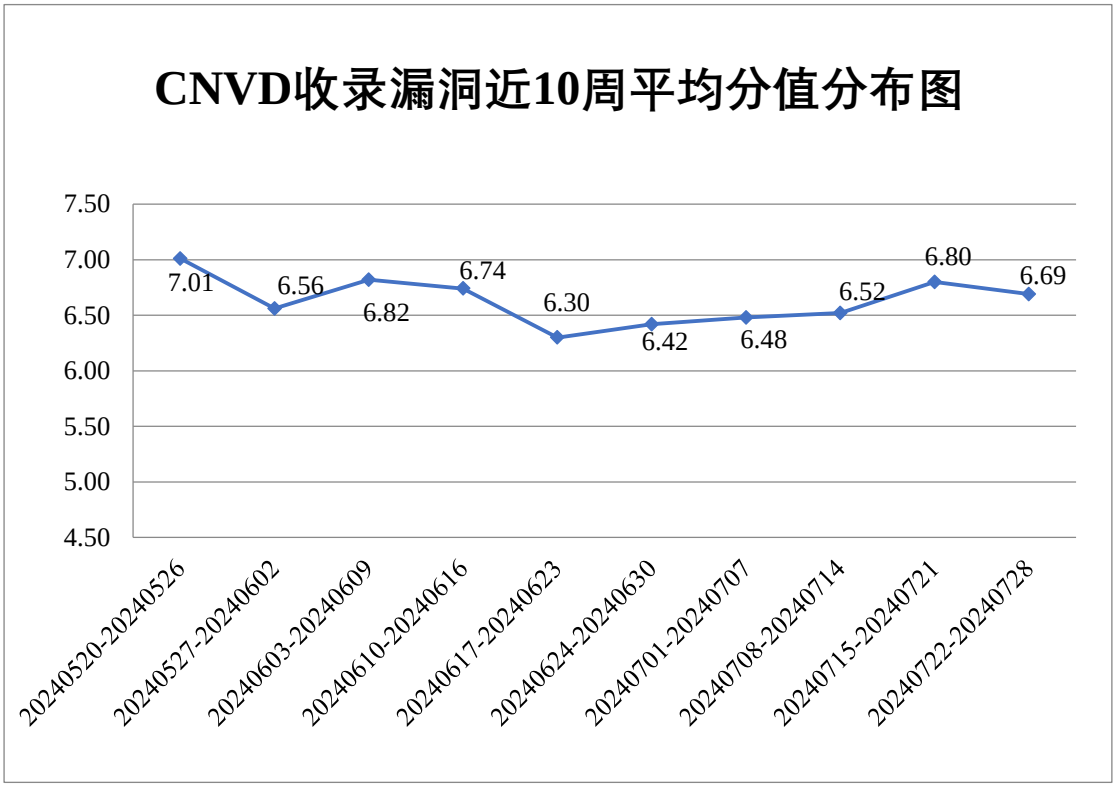

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 6 起，向基础电信企业通报漏洞事件 3 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 503 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 27 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 10 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、中科数字通（北京）科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、耘申信息科技（上海）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、星云海数字科技股份有限公司、新天科技股份有限公司、新开普电子股份有限公司、夏普科技（上海）有限公司、武汉中地数码科技有限公司、泰雷兹（中国）企业管理有限公司、台达电子企业管理（上海）有限公司、苏州美名软件有限公司、施耐德电气（中国）有限公司、深圳市同享软件科技有限公司、深圳市蓝凌软件股份有限公司、深圳市科荣软件股份有限公司、深圳市飞速创新技术股份有限公司、深圳市必联电子有限公司、深圳市爱施德股份有限公司、深圳极速创想科技有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海上讯信息技术股份有限公司、上海金慧软件有限公司、上海泛微网络科技股份有限公司、上海布雷德科技有限公司、上海博达数据通信有限公司、熵基科技股份有限公司、山东金钟科技集团股份有限公司、南京帆软软件有限公司、迈普通信技术股份有限公司、利盟信息技术（中国）有限公司、理光（中国）投资有限公司、朗坤智慧科技股份有限公司、柯尼卡美能达集团、京信通信技术（广州）有限公司、佳能（中国）有限公司、洪湖尔创网联信息技术有限公司、恒信汽车集团股份有限公司、杭州雄伟科技开发股份有限公司、杭州安恒信息技术股份有限公司、广州华壹智能科技有限公司、广联达科技股份有限公司、广东保伦电子股份有限公司、富士施乐（中国）有限公司、福建星网锐捷通讯股份有限公司、东芝（中国）有限公司、大唐电信科技股份有限公司、成都任我行软件股份有限公司、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、北京星网锐捷网络技术有限公司、北京通达信科科技有限公司、北京神州视翰科技有限公司、北京人大金仓信息技术股份有限公司、北京勤哲软件技术有限责任公司、北京金和网络股份有限公司、北京海睿兴业科技有限公司、北京达美嘉教育科技有限公司、百度安全应急响应中心、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、安歌科技（集团）股份有限公司、阿里巴巴集团安全应急响应中心和 NEC。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、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。河南东方云盾信息技术有限公司、重庆都会信息科技、江苏金盾检测技术股份有限公司、上海直画科技有限公司、成都卫士通信息安全技术有限公司、快页信息技术有限公司、北京远禾科技有限公司、江苏百达智慧网络科技有限公司、中资网络信息安全科技有限公司、亚信科技（成都）有限公司、联想集团及其他个人白帽子向 CNVD 提交了 54241 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、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 53817 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）	39530	39530
奇安信网神（补天平台）	13730	13730
北京启明星辰信息安全技术有限公司	627	0
新华三技术有限公司	529	0
安天科技集团股份有限公司	461	0
三六零数字安全科技集团有限公司	349	349
上海交大	208	208
北京天融信网络安全技术有限公司	183	0
杭州安恒信息技术股份有限公司	166	3
阿里云计算有限公司	165	0
恒安嘉新（北京）科技股份公司	92	0
深信服科技股份有限公司	58	0
北京知道创宇信息技术有限公司	36	0
杭州迪普科技股份有限公司	30	0

北京数字观星科技有限公司	20	0
南京众智维信息科技有限公司	19	19
北京安信天行科技有限公司	19	19
北京知道创宇信息技术有限公司	4	0
北京长亭科技有限公司	3	1
北京升鑫网络科技有限公司（青藤云）	1	1
河南东方云盾信息技术有限公司	15	15
重庆都会信息科技	10	10
江苏金盾检测技术股份有限公司	4	4
上海直画科技有限公司	4	4
成都卫士通信息安全技术有限公司	3	3
西门子（中国）有限公司	3	0
快页信息技术有限公司	2	2
北京远禾科技有限公司	1	1
江苏百达智慧网络科技有限公司	1	1
中资网络信息安全科技有限公司	1	1
亚信科技（成都）有限公司	1	1
联想集团	1	1
CNCERT 贵州分中心	1	1

个人	337	337
报送总计	56614	54241

本周漏洞按类型和厂商统计

本周，CNVD 收录了 223 个漏洞。应用程序 131 个，WEB 应用 45 个，网络设备（交换机、路由器等网络端设备）43 个，操作系统 4 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	131
WEB 应用	45
网络设备（交换机、路由器等网络端设备）	43
操作系统	4

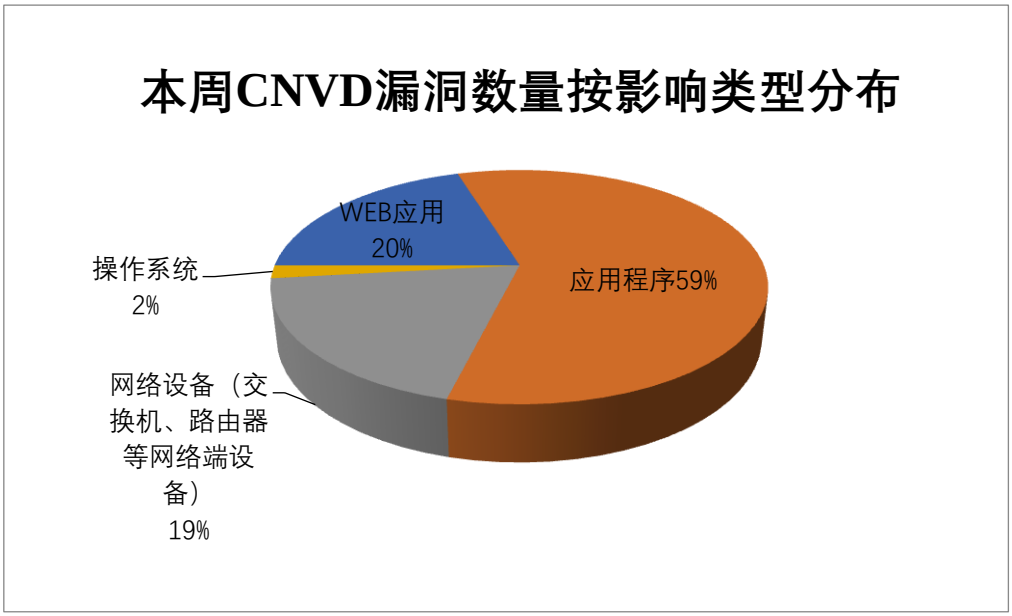

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 PDF-XChange、Kofax、D-Link 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	PDF-XChange	43	19%
2	Kofax	40	18%
3	D-Link	26	12%
4	Google	16	7%
5	Ruvar	15	7%
6	IBM	14	6%

7	LG	11	5%
8	NETGEAR	10	5%
9	Adobe	9	4%
10	其他	39	17%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，1 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Tenda O3 fromVirtualSet 函数缓冲区溢出漏洞（CNVD-2024-33692）、D-Link DAP-1360 栈缓冲区溢出漏洞（CNVD-2024-33377）”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/

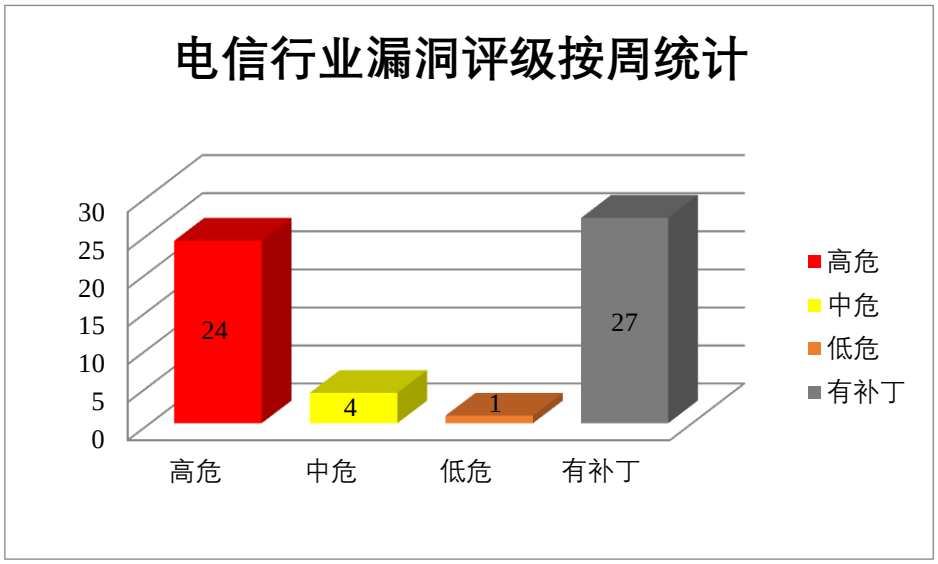

图 3 电信行业漏洞统计

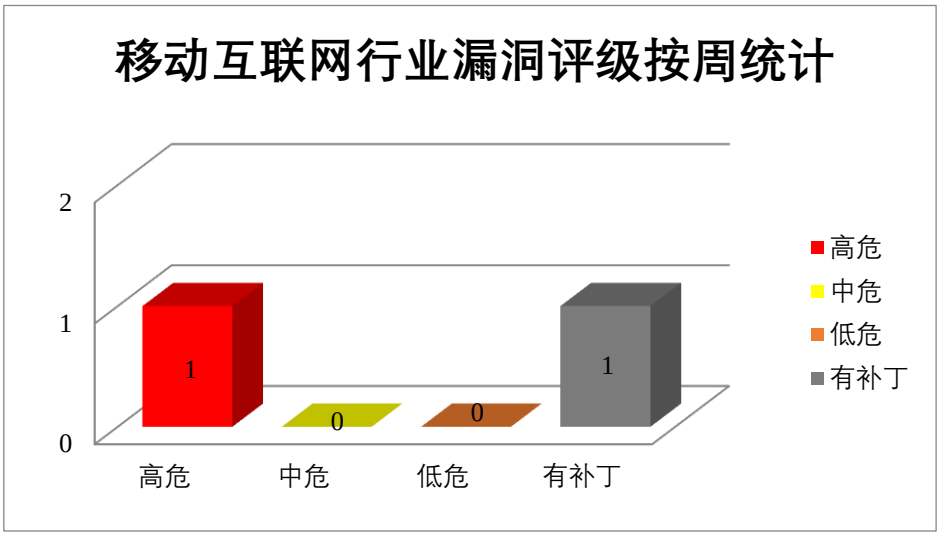

图 4 移动互联网行业漏洞统计

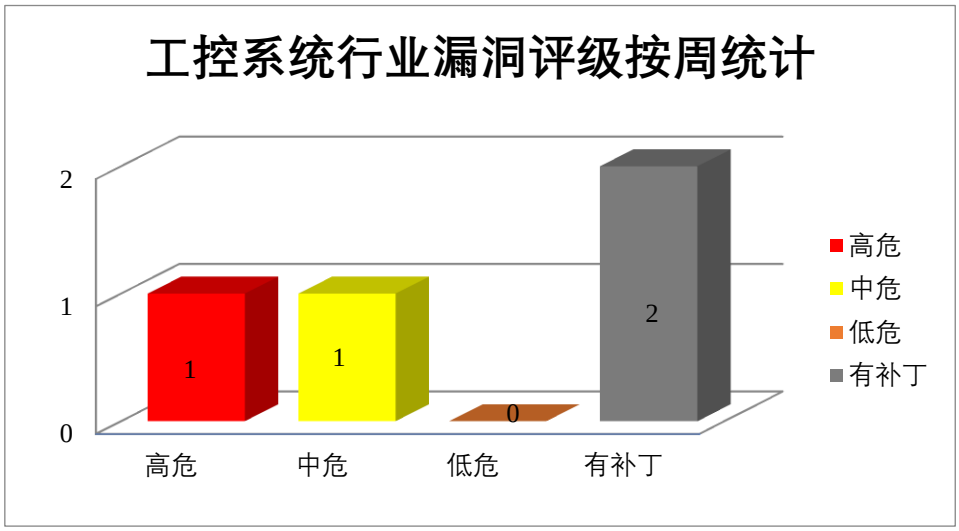

图 5 工控系统行业漏洞统计

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 Datacap Navigator 是美国国际商业机器（IBM）公司的一个用于 Datacap 的 Web 客户机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞收集信息，在 Web UI 中嵌入任意 JavaScript 代码，通过特制 URL 请求来查看系统上的任意文件等。

CNVD 收录的相关漏洞包括：IBM Datacap Navigator 跨站脚本漏洞、IBM Datacap Navigator 信息泄露漏洞（CNVD-2024-33363、CNVD-2024-33366、CNVD-2024-33368、CNVD-2024-33371）、IBM Datacap Navigator 加密问题漏洞、IBM Datacap Navigator 服务器端请求伪造漏洞、IBM Datacap Navigator 路径遍历漏洞。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-2024-33364

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33363

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33362

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33368

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33367

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33366

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33365

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33371

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。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，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2024-33609、CNVD-2024-33601、CNVD-2024-33602、CNVD-2024-33604、CNVD-2024-33603、CNVD-2024-33606）、Google Chrome 代码执行漏洞（CNVD-2024-33605、CNVD-2024-33607）。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-2024-33601

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33602

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33604

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33603

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33606

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33605

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33607

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33609

3、 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-2024-33385、CNVD-2024-33384、CNVD-2024-33383、CNVD-2024-33387、CNVD-2024-33386、CNVD-2024-33390、CNVD-2024-33392、CNVD-2024-33391）。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-2024-33385
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33384
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33383
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33387
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33386
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33390
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33392
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33391

4、Apache 产品安全漏洞

Apache StreamPark 是美国阿帕奇（Apache）基金会的一个流媒体应用程序开发框架。Apache Airflow 是美国阿帕奇（Apache）基金会的一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。Apache Linkis 是美国阿帕奇（Apache）基金会的一款中间件产品，可以在上层应用和底层数据引擎之间建立起有效的连接。Apache StreamPipes 是美国阿帕奇（Apache）基金会的一个自助式（工业）物联网工具箱，使非技术用户能够连接、分析和探索 IIoT 数据流。Apache CloudStack 是美国阿帕奇（Apache）基金会的一套基础架构即服务（IaaS）云计算平台。该平台主要用于部署和管理大型虚拟机网络。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在 DataSource Manager Module 中配置恶意的 db2 参数将导致 jndi 注入，将恶意脚本注入 Web 页面，窃取受害者的基于 cookie 的身份验证凭据，插入命令进行远程命令执行。

CNVD 收录的相关漏洞包括：Apache StreamPark 命令注入漏洞（CNVD-2024-33577、CNVD-2024-33576）、Apache Airflow 代码执行漏洞（CNVD-2024-33592）、Apache Airflow 存在跨站脚本漏洞、Apache Linkis 代码问题漏洞（CNVD-2024-33595、CNVD-2024-33596）、Apache StreamPipes 安全特征问题漏洞、Apache CloudStack 代码注入漏洞。其中，除“Apache StreamPark 命令注入漏洞（CNVD-2024-33576、CNVD-2024-33577）、Apache Airflow 存在跨站脚本漏洞”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-2024-33577
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33576
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33592
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33591
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33595
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33596
https://www.cnvd.org.cn/flaw/show/CNVD-2024-33598

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33597

5、TOTOLINK A3700R setIpPortFilterRules 函数缓冲区溢出漏洞

TOTOLINK A3700R 是中国吉翁电子（TOTOLINK）公司的一款无线路由器。本周，TOTOLINK A3700R 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-2024-33694

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-2024-33377	D-Link DAP-1360 栈缓冲区溢出漏洞（CNVD-2024-33377）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
CNVD-2024-33376	D-Link DAP-1360 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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
CNVD-2024-33375	D-Link DAP-1360 硬编码身份认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
CNVD-2024-33381	D-Link DAP-1360 栈缓冲区溢出漏洞（CNVD-2024-33381）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
CNVD-2024-33380	D-Link DAP-1360 栈缓冲区溢出漏洞（CNVD-2024-33380）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
CNVD-2024-33379	D-Link DAP-1360 栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.asp

			x?name=SAP10324
CNVD-2024-33378	D-Link DAP-1360 栈缓冲区溢出漏洞（CNVD-2024-33378）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
CNVD-2024-33382	D-Link DAP-1360 栈缓冲区溢出漏洞（CNVD-2024-33382）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
CNVD-2024-33400	D-Link DIR-2150 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.dlink.com/
CNVD-2024-33403	SeaCMS admin_weixin.php 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://www.seacms.net/

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞收集信息，在 Web UI 中嵌入任意 JavaScript 代码，通过特制 URL 请求来查看系统上的任意文件。此外，Google、Adobe、Apache 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，在系统上执行任意代码，注入精心设计的有效载荷执行任意 Web 脚本或 HTML，在 DataSource Manager Module 中配置恶意的 db2 参数将导致 jndi 注入，将恶意脚本注入 Web 页面，窃取受害者的基于 cookie 的身份验证凭据，插入命令进行远程命令执行等。另外，TOTOLINK A3700R 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、Opencart 跨站请求伪造漏洞（CNVD-2024-33388）

验证描述

Opencart 是中国 Opencart 公司的一套开源的电子商务系统。该系统提供产品评论、产品评分、产品添加等模块。

Opencart 3.0.3.6 版本存在跨站请求伪造漏洞，该漏洞源于 WEB 应用未充分验证请求是否来自可信用户，攻击者可利用该漏洞通过 add to cart 添加购物车物品。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49228

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-33388

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. OpenStack Nova 漏洞允许黑客未经授权访问云服务器

该漏洞被跟踪为 CVE-2024-40767，影响了 Nova 的多个版本，并对全球云基础设施构成严重风险。

参考链接：https://cybersecuritynews.com/openstack-nova-vulnerability/

2. 网络攻击者在窃取活动中利用 Microsoft SmartScreen 漏洞

于 2 月份修补的 Microsoft Defender SmartScreen 漏洞仍在全球范围内用于信息窃取攻击，Fortinet 标记了两个攻击者：Meduza 和 ACR，到目前为止，攻击范围已包括美国、西班牙和泰国。

参考链接：https://www.darkreading.com/vulnerabilities-threats/cyberattackers-exploit-microsoft-smartscreen-bug-in-stealer-campaign

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