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 01 日-2024 年 07 月 07 日 **2024 年第 27 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 285 个，其中高危漏洞 143 个、中危漏洞 123 个、低危漏洞 19 个。漏洞平均分值为 6.48。本周收录的漏洞中，涉及 0day 漏洞 180 个（占 63 %），其中互联网上出现“JFinalCMS 跨站脚本漏洞（CNVD-2024-30065）、Employee Management System SQL 注入漏洞（CNVD-2024-30066）”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 17463 个，与上周（16683 个）环比增加 5%。

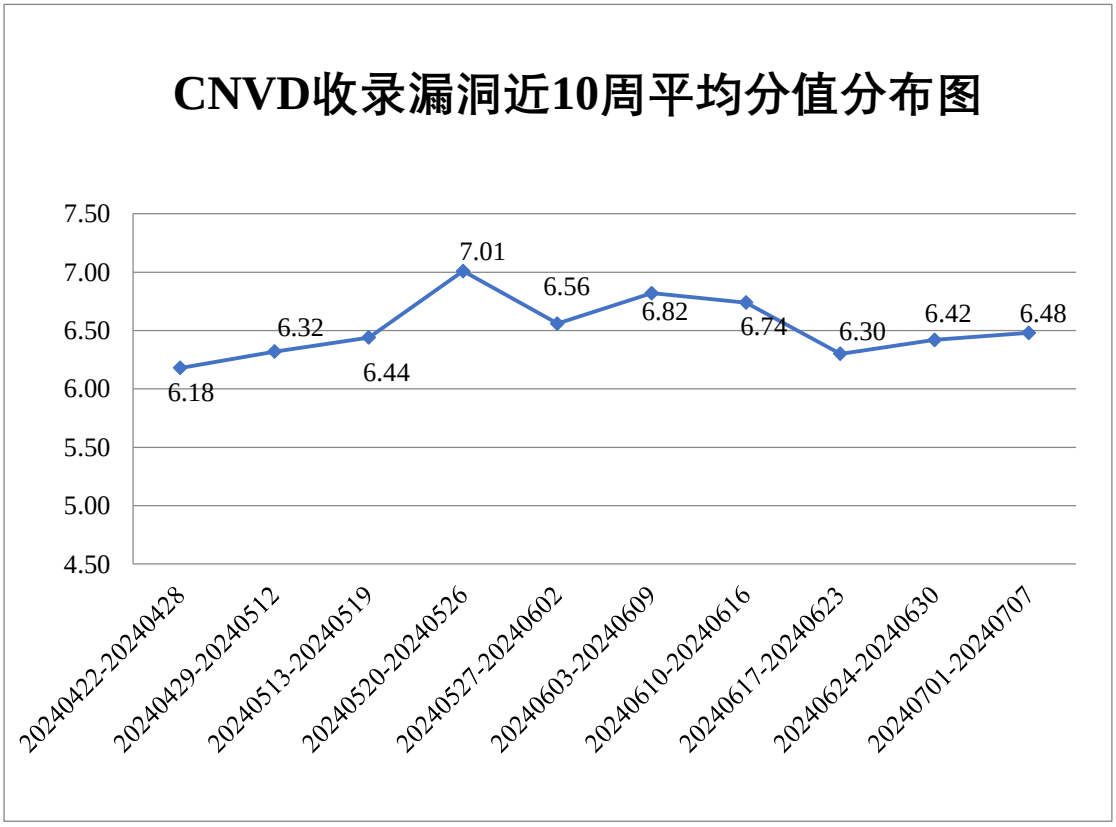

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 9 起，向基础电信企业通报漏洞事件 5 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 785 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 109 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 22 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、卓智网络科技有限公司、珠海金山办公软件有限公司、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、用友网络科技股份有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、西门子（中国）有限公司、西安华谊云信息科技有限公司、西安城投新能源有限责任公司、武汉天地伟业科技有限公司、武汉三佳医疗信息技术有限公司、无锡路通视信网络股份有限公司、卫宁健康科技集团股份有限公司、万洲电气股份有限公司、天阳科技（集团）有限公司、天津神舟通用数据技术有限公司、索尼（中国）有限公司、深圳智慧光迅信息技术有限公司、深圳万广互联科技有限公司、深圳拓安信物联股份有限公司、深圳市中科网威科技有限公司、深圳市造物数字工业科技有限公司、深圳市维斯易联科技有限公司、深圳市天地心网络技术有限公司、深圳市赛格导航科技股份有限公司、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、申瓯通信设备有限公司、上海桑锐电子科技股份有限公司、上海荃路软件开发工作室、上海启略网络科技有限公司、上海普加软件有限公司、上海鹏达计算机系统开发有限公司、上海肯特仪表股份有限公司、上海华测导航技术股份有限公司、上海发那科机器人有限公司、上海爱数信息技术股份有限公司、山西牛之云网络科技有限公司、山东潍微科技股份有限公司、山东宏信化工股份有限公司、厦门商集网络科技有限责任公司、厦门科拓通讯技术股份有限公司、三星（中国）投资有限公司、青岛浩海网络科技股份有限公司、青岛海威茨仪表有限公司、麒麟软件有限公司、南京星远图科技有限公司、南京科远智慧科技集团股份有限公司、力合科技（湖南）股份有限公司、柯尼卡美能达（中国）投资有限公司、京瓷办公信息系统（中国）有限公司、锦翰科技（深圳）有限公司、金华迪加网络科技有限公司、江苏麦维智能科技有限公司、江苏麦克思软件有限公司、佳能（中国）有限公司、济南政和科技有限公司、吉翁电子（深圳）有限公司、黑龙江威速科技有限公司、河北先河环保科技股份有限公司、杭州展之信息技术有限公司、杭州云润科技有限公司、杭州炫方网络技术有限公司、杭州三汇数字信息技术有限公司、杭州海康威视数字技术股份有限公司、瀚高基础软件股份有限公司、广州众米信息科技有限公司、广州致翔计算机科技有限公司、广州市璐华计算机有限公司、广州市保伦电子有限公司、广联达科技股份有限公司、广东保伦电子股份有限公司、富士胶片商业创新（中国）有限公司、福建科

立讯通信有限公司、飞利达科技股份有限公司、飞救医疗科技（北京）有限公司、泛微网络科技股份有限公司、帆软软件有限公司、东集技术股份有限公司、东莞市通天星软件科技有限公司、鼎捷软件股份有限公司、成都比格图数据处理有限公司、畅捷通信息技术股份有限公司、北京中远麒麟科技有限公司、北京中农信达信息技术有限公司、北京智云达科技股份有限公司、北京赢科天地电子有限公司、北京英视睿达科技股份有限公司、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、北京五指互联科技有限公司、北京数字政通科技股份有限公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京润乾信息系统技术有限公司、北京人大金仓信息技术股份有限公司、北京久其软件股份有限公司、北京金和网络股份有限公司、北京慧图科技（集团）股份有限公司、北京华清信安科技有限公司、北京汉邦高科数字技术股份有限公司、北京邦永科技有限公司、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、奥琦玮信息科技（北京）有限公司、安翼物联网（南京）有限公司、安美世纪（北京）科技有限公司、安徽旭帆信息科技有限公司、安徽生命港湾信息技术有限公司、安歌科技（集团）股份有限公司、爱普生（中国）有限公司、seacms、OPPO 广东移动通信有限公司和 ABB。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天津市国瑞数码安全系统股份有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司、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。江苏金盾检测技术股份有限公司、快页信息技术有限公司、河南东方云盾信息技术有限公司、北京山石网科信息技术有限公司、江苏晟晖信息科技有限公司、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、南京深安科技有限公司、上海直画科技有限公司、厦门聚丁科技有限公司、安徽天行网安信息安全技术有限公司、中国电信股份有限公司上海研究院、中孚安全技术有限公司、江苏极元信息技术有限公司、成都久信信息技术股份有限公司、北京翰慧投资咨询有限公司、上海观安信息技术股份有限公司、甘肃赛飞安全科技有限公司、中华人民共和国上海海事局、北京天防安全科技有限公司、杭州默安科技有限公司、含光实验室、深圳市魔方安全科技有限公司及其他个人白帽子向 CNVD 提交了 17463 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 16457 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	11296	11296

台）		
斗象科技（漏洞盒子）	3400	3400
三六零数字安全科技集团有限公司	1355	1355
天津市国瑞数码安全系统股份有限公司	712	0
新华三技术有限公司	543	0
上海交大	406	406
北京神州绿盟科技有限公司	347	0
安天科技集团股份有限公司	225	0
北京数字观星科技有限公司	218	0
阿里云计算有限公司	164	0
恒安嘉新（北京）科技股份公司	62	0
北京启明星辰信息安全技术有限公司	55	0
远江盛邦（北京）网络安全科技股份有限公司	50	50
华为技术有限公司	49	0
北京知道创宇信息技术有限公司	41	0
杭州安恒信息技术股份有限公司	32	22
北京安信天行科技有限公司	18	18
杭州迪普科技股份有限公司	10	0
北京天融信网络安全技术有限公司	6	6
南京众智维信息科技有限公司	3	3

江苏金盾检测技术股份有限公司	55	55
快页信息技术有限公司	36	36
河南东方云盾信息技术有限公司	24	24
北京山石网科信息技术有限公司	12	12
江苏晟晖信息科技有限公司	7	7
马鞍山书拓安全科技有限公司	4	4
江苏云天网络安全技术有限公司	3	3
南京深安科技有限公司	3	3
上海直画科技有限公司	3	3
厦门聚丁科技有限公司	3	3
安徽天行网安信息安全技术有限公司	2	2
中国电信股份有限公司上海研究院	2	2
中孚安全技术有限公司	2	2
江苏极元信息技术有限公司	2	2
成都久信信息技术股份有限公司	2	2
北京翰慧投资咨询有限公司	2	2
上海观安信息技术股份有限公司	1	1
甘肃赛飞安全科技有	1	1

限公司		
中华人民共和国上海海事局	1	1
北京天防安全科技有限公司	1	1
杭州默安科技有限公司	1	1
含光实验室	1	1
深圳市魔方安全科技有限公司	1	1
CNCERT 贵州分中心	1	1
个人	737	737
报送总计	19899	17463

本周漏洞按类型和厂商统计

本周，CNVD 收录了 285 个漏洞。按类型划分包括 WEB 应用 150 个，应用程序 76 个，网络设备（交换机、路由器等网络端设备）27 个，操作系统 15 个，智能设备（物联网终端设备）10 个，数据库 5 个，安全产品 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	150
应用程序	76
网络设备（交换机、路由器等网络端设备）	27
操作系统	15
智能设备（物联网终端设备）	10
数据库	5
安全产品	2

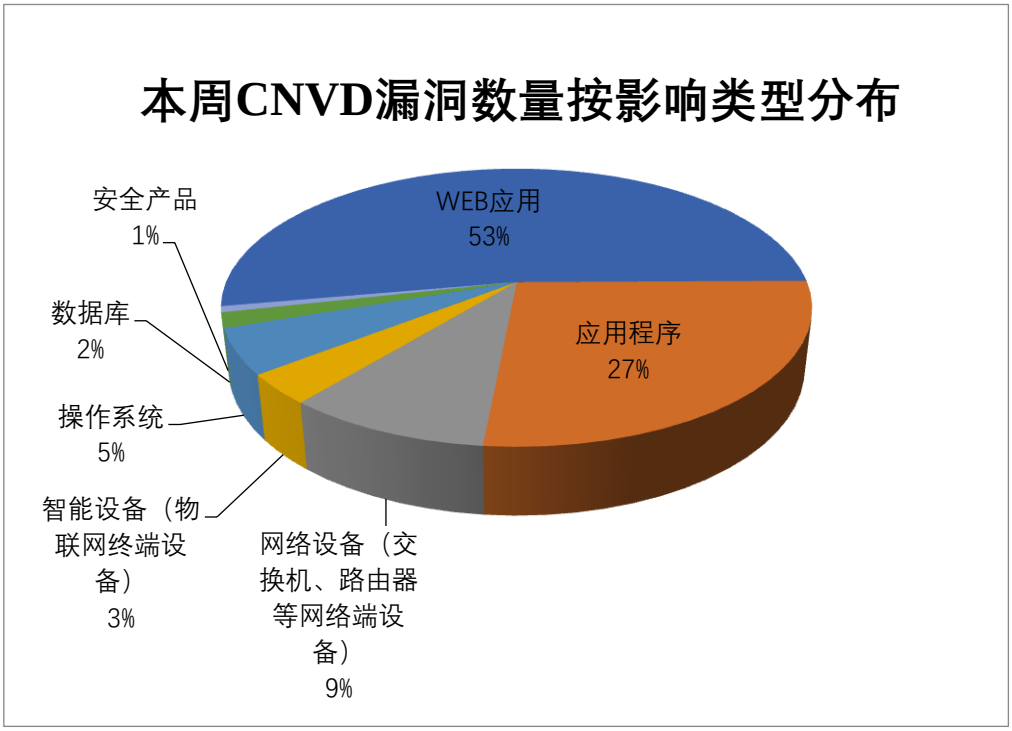

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、FFmpeg、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	Adobe	24	8%
2	FFmpeg	13	5%
3	IBM	12	4%
4	Linux	10	4%
5	用友网络科技股份有限公司	9	3%
6	Foxit	9	3%
7	Cybozu	8	3%
8	北京百卓网络技术有限公司	6	2%
9	福建科立讯通信有限公司	6	2%
10	其他	188	66%

本周行业漏洞收录情况

本周，CNVD 收录了 21 个电信行业漏洞，8 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“OpenSSH 远程代码执行漏洞（CNVD-2024-29805）、Rockwell Automation Arena Simulation Software 缓冲区溢出漏洞（CNVD-2024-30639）”

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/

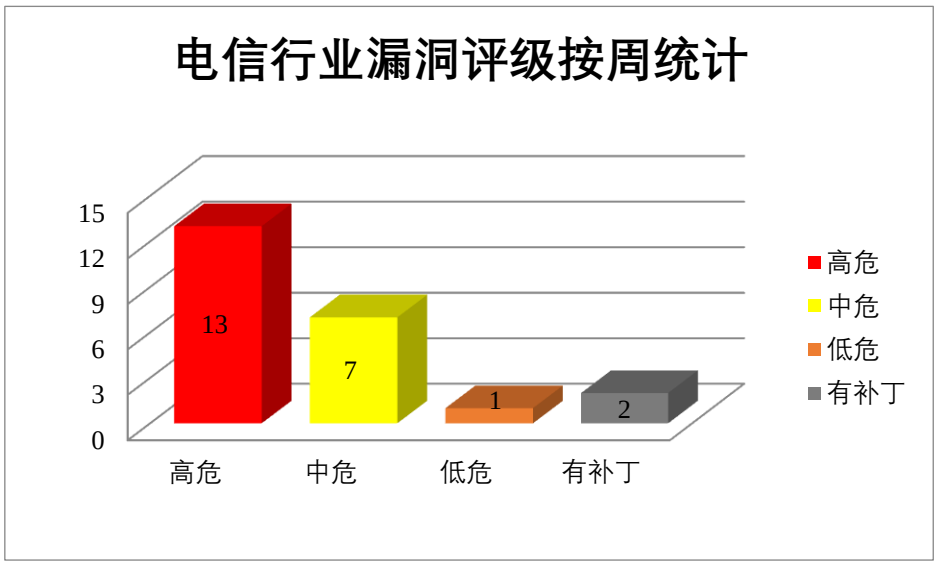

图 3 电信行业漏洞统计

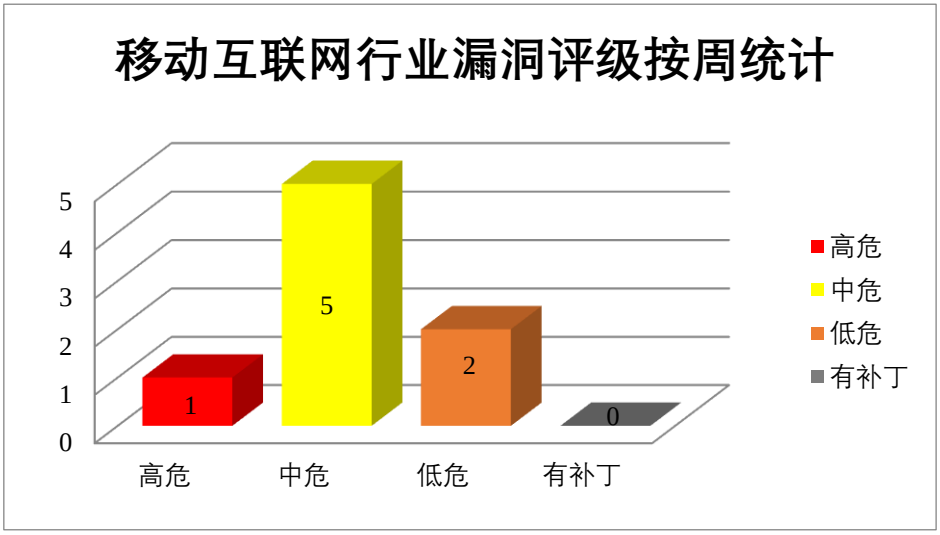

图 4 移动互联网行业漏洞统计

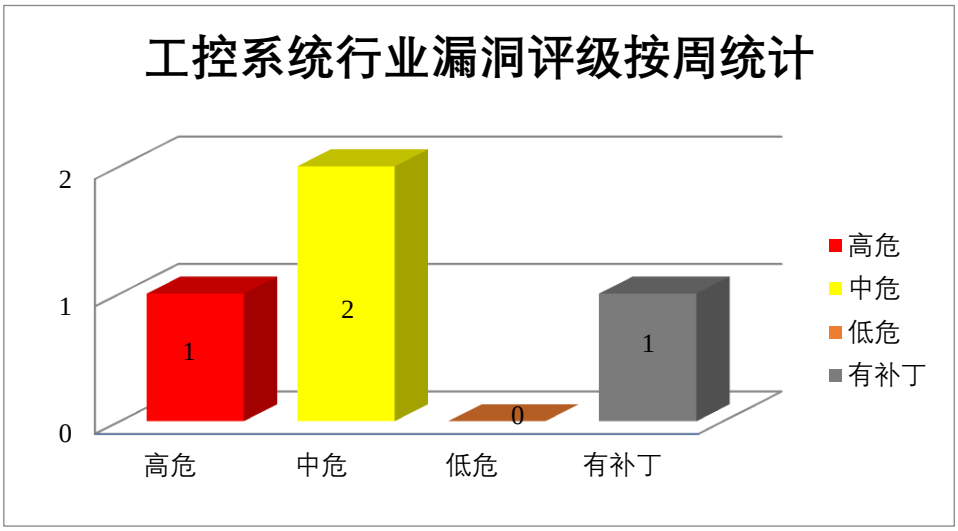

图 5 工控系统行业漏洞统计

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 Cognos Analytics 是美国国际商业机器（IBM）公司的一套商业智能软件。该软件包括报表、仪表板和记分卡等，并可通过分析关键因素与关键人等内容，协助企业调整决策。IBM Sterling B2B Integrator 是美国国际商业机器（IBM）公司的一套集成了重要的 B2B 流程、交易和关系的软件。该软件支持与不同的合作伙伴社区之间实现复杂的 B2B 流程的安全集成。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 IBM WebSphere 软件平台的基础。IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。IBM i 是美国国际商业机器（IBM）公司的一套运行在 IBM Power Systems 和 IBM PureSystems 中的操作系统。IBM Security Access Manager 是美国国际商业机器（IBM）公司的一款应用于信息安全管理的产品。该产品通过面向 Web、移动和云计算的集成设备来实现访问管理控制。IBM Cloud Pak for Security 是美国国际商业机器（IBM）公司的一款应用软件。一个开放的安全平台，可连接到您现有的数据源以产生更深刻的见解，并使您能够更快地采取自动化行动。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，在 Web UI 中嵌入任意 JavaScript 代码，从而导致受信任会话中的凭据泄露，执行恶意命令等。

CNVD 收录的相关漏洞包括：IBM Cognos Analytics 跨站脚本漏洞（CNVD-2024-30212）、IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2024-30211）、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2024-30215）、IBM InfoSphere Info

rmation Server 跨站脚本漏洞（CNVD-2024-30214）、IBM InfoSphere Information Server 跨站请求伪造漏洞（CNVD-2024-30213）、IBM i 权限许可和访问控制问题漏洞（CNVD-2024-30218）、IBM Security Access Manager 加密问题漏洞（CNVD-2024-30216）、IBM Cloud Pak for Security 信息泄露漏洞（CNVD-2024-30219）。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-2024-30212
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30211
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30215
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30214
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30213
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30218
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30216
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30219

2、 Foxit 产品安全漏洞

Foxit PDF Reader 是中国福昕（Foxit）公司的一款 PDF 阅读器。Foxit PDF Editor 是中国福昕（Foxit）公司的一款 PDF 编辑器。本周，上述产品被披露存在多个漏洞，攻击者可利用在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PDF Reader and Foxit PDF Editor 代码执行漏洞（CNVD-2024-29751、CNVD-2024-29754、CNVD-2024-29753、CNVD-2024-29752、CNVD-2024-29758、CNVD-2024-29757、CNVD-2024-29756、CNVD-2024-29755）。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-2024-29751
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29754
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29753
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29752
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29758
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29757
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29756
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29755

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多个漏洞，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-2024-30048、CNVD-2024-30047、CNVD-2024-30046、CNVD-2024-30045、CNVD-2024-30051、CNVD-2024-30050、CNVD-2024-30049、CNVD-2024-30053）。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-2024-30048
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30047
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30046
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30045
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30051
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30050
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30049
https://www.cnvd.org.cn/flaw/show/CNVD-2024-30053

4、Cybozu 产品安全漏洞

Cybozu Garoon 是日本才望子（Cybozu）公司的一套门户型 OA 办公系统。该系统提供门户、E-mail、书签、日程安排、公告栏、文件管理等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞删除 Shared to Dos 的数据，更改、获取 Memo 的数据，通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cybozu Garoon 安全绕过漏洞（CNVD-2024-29666、CNVD-2024-29667）、Cybozu Garoon 拒绝服务漏洞（CNVD-2024-29668）、Cybozu Garoon 信息泄露漏洞（CNVD-2024-29669、CNVD-2024-29670、CNVD-2024-29673）、Cybozu Garoon 跨站脚本漏洞（CNVD-2024-29671）、Cybozu Garoon 资源管理错误漏洞。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-2024-29666
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29667
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29668
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29669
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29670
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29671
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29672
https://www.cnvd.org.cn/flaw/show/CNVD-2024-29673

5、TP-LINK ER7206 命令执行漏洞

TP-LINK ER7206 是中国普联（TP-LINK）公司的一款多功能千兆路由器。本周，

TP-LINK ER7206 被披露存在命令执行漏洞。攻击者可利用该漏洞通过特制的网络请求可导致任意命令执行。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-2024-30632

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-2024-29674	FFmpeg 缓冲区溢出漏洞（CNVD-2024-29674）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://trac.ffmpeg.org/ticket/10746
CNVD-2024-29676	FFmpeg 缓冲区溢出漏洞（CNVD-2024-29676）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://trac.ffmpeg.org/ticket/10738
CNVD-2024-29675	FFmpeg 缓冲区溢出漏洞（CNVD-2024-29675）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://trac.ffmpeg.org/ticket/10743
CNVD-2024-29677	FFmpeg 缓冲区溢出漏洞（CNVD-2024-29677）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://trac.ffmpeg.org/ticket/10699
CNVD-2024-29679	FFmpeg 缓冲区溢出漏洞（CNVD-2024-29679）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://trac.ffmpeg.org/ticket/10701
CNVD-2024-30067	OpenCart 授权问题漏洞（CNVD-2024-30067）	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/opencart/opencart
CNVD-2024-30072	OpenCart SQL 注入漏洞（CNVD-2024-30072）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.snyk.io/vuln/SNYK-PHP-OPENCARTOPENCART-7266565
CNVD-2024-30085	GeoServer 远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://geoserver.org/
CNVD-2024-30374	Linux kernel 代码执行漏洞（CNVD-2024-30374）	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.kernel.org/
CNVD-2024-30634	Google Chrome 资源管理错误漏洞（CNVD-2024-30634）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/06/stable-channel-update-for-

			desktop_18.html

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，在 Web UI 中嵌入任意 JavaScript 代码，从而导致受信任会话中的凭据泄露，执行恶意命令等。此外，Foxit、Adobe、Cybozu 等多款产品被披露存在多个漏洞，攻击者可利用漏洞注入精心设计的有效载荷执行任意 Web 脚本或 HTML，在系统上执行任意代码等。另外，TP-LINK ER7206 被披露存在命令执行漏洞。攻击者可利用漏洞通过特制的网络请求可导致任意命令执行。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、JFinalCMS 跨站脚本漏洞（CNVD-2024-30065）

验证描述

JFinalCMS 是一个内容管理系统。

JFinalCMS 20240111 及之前版本存在跨站脚本漏洞，该漏洞源于文件/admin/template 的参数 directory 存在跨站脚本（XSS）漏洞。攻击者可利用该漏洞注入恶意指令代码到网页。

验证信息

POC 链接：https://gitee.com/heyewei/JFinalcms/issues/I8VHGR

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-30065

信息提供者

恒安嘉新（北京）科技股份公司

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. macOS 版 ChatGPT 被指以纯文本存储 AI 对话，OpenAI 紧急更新修复

由于对话是以纯文本形式存储在沙盒之外，这也意味着在用户不知情的情况下，对话可以被 Mac 上运行的其他应用程序、进程甚至恶意软件访问。

参考链接：https://www.ithome.com/0/779/522.htm

2. 100 亿条密码汇编集合 RockYou2024 泄露，酿成史上最大密码泄露事件

RockYou2024 密码汇编集合里包含世界各地个人使用的真实密码。研究人员认为，

黑客将数量如此庞大的密码泄露出去，大大增加了凭证填充攻击的风险。

参考链接：https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/

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