国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 03 月 25 日-2024 年 03 月 31 日 **2024 年第 13 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 394 个，其中高危漏洞 154 个、中危漏洞 223 个、低危漏洞 17 个。漏洞平均分值为 6.25。本周收录的漏洞中，涉及 0day 漏洞 282 个（占 72%），其中互联网上出现“magicflue 文件上传漏洞、DzzOffice 跨站脚本漏洞（CNVD-2024-15545）”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 11801 个，与上周（5953 个）环比增加 98%。

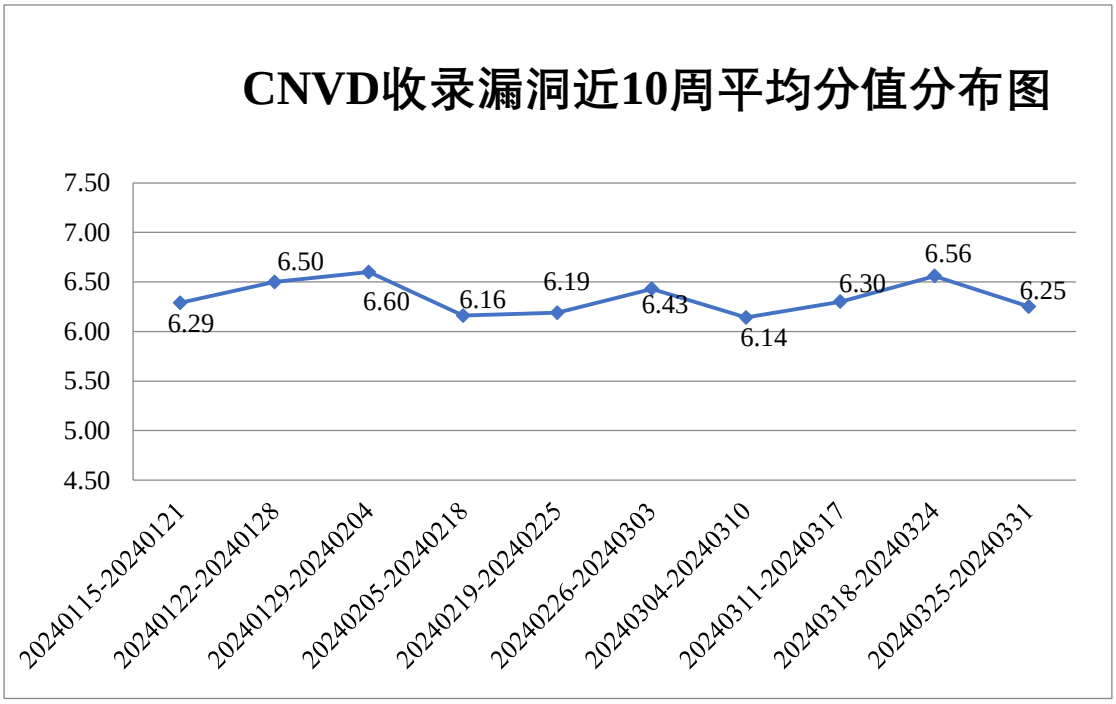

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 12 起，向基础电

信企业通报漏洞事件 16 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 489 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 91 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 30 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：

北京星网锐捷网络技术有限公司、佐藤自动识别系统国际贸易（上海）有限公司、珠海金山办公软件有限公司、珠海海鸟科技有限公司、重庆中联信息产业有限责任公司、重庆梅安森科技股份有限公司、中控技术股份有限公司、中科方德软件有限公司、智邦大陆科技有限公司、正方软件股份有限公司、浙江和达科技股份有限公司、浙江浩腾电子科技股份有限公司、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、新都（青岛）办公系统有限公司、孝感柏仁信息技术有限公司、夏普商贸（中国）有限公司、西门子（中国）有限公司、西安大西信息科技有限公司、武汉海昌信息技术有限公司、武汉达梦数据库有限公司、武汉城投停车场投资建设管理有限公司、万洲电气股份有限公司、天津市天科数创科技股份有限公司、天津鸿软通联信息技术有限公司、天津红日药业股份有限公司、台达电子企业管理（上海）有限公司、宿迁鑫潮信息技术有限公司、苏州伟创电气科技股份有限公司、苏州华兆科技有限公司、四平市九州易通科技有限公司、四川易泊时捷智能科技有限公司、世邦通信股份有限公司、深圳拓安信物联股份有限公司、深圳市月歌科技有限公司、深圳市同享软件科技有限公司、深圳市思源计算机软件股份有限公司、深圳市企慧通信息技术有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔联科科技有限公司、深圳市博思协创网络科技有限公司、深圳力维智联技术有限公司、申瓯通信设备有限公司、上海瑞策软件有限公司、上海迈微软件科技有限公司、上海寰创通信科技股份有限公司、上海汉得信息技术股份有限公司、上海泛微网络科技股份有限公司、上海达彩数据科技有限公司、上海博达数据通信有限公司、商派软件有限公司、山西森甲能源科技有限公司、山脉科技股份有限公司、山东潍微科技股份有限公司、山东商行天下软件科技有限公司、山东金钟科技集团股份有限公司、厦门亿联网络技术股份有限公司、厦门新控网络科技有限责任公司、厦门四信通信科技有限公司、若依、青岛三利集团有限公司、青岛聚城网络科技有限公司、青岛海信网络科技股份有限公司、启业云大数据（南京）有限公司、南宁小橙科技有限公司、南京帆软软件有限公司、南昌航天广信科技有限责任公司、陌创有限公司、绵阳探云科技有限公司、迈普通信技术股份有限公司、龙芯中科技术股份有限公司、龙采科技集团有限责任公司、联想集团、蓝网科技股份有限公司、柯尼卡美能达办公系统（中国）有限公司、金蝶软件（中国）有限公司、江苏金智教育信息股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华讯高科股份有限公司、华硕电脑股份有限公司、湖南强智科技发展有限公司、河北子午云网络科技有限

公司、河北先河环保科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州三汇信息工程有限公司、杭州蓝代斯克数字技术有限公司、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、杭州恩软信息技术有限公司、翰威通信有限公司、广州唯众网络科技有限公司、广州图创计算机软件开发有限公司、广州市溢信科技股份有限公司、广州市花都区新华伟创广告设计服务部、广州市保伦电子有限公司、广州恒企教育科技有限公司、广东新禾道信息科技有限公司、福建科立讯通信有限公司、福建汇川物联网技术科技股份有限公司、佛山市华跃计算机系统有限公司、成都智蜂网科技有限责任公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、北京中农信达信息技术有限公司、北京中科聚网信息技术有限公司、北京中成科信科技发展有限公司、北京智邦国际软件技术有限公司、北京致远互联软件股份有限公司、北京用友政务软件股份有限公司、北京亚控科技发展有限公司、北京新网医讯技术有限公司、北京网康科技有限公司、北京万户软件技术有限公司、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、北京派网软件有限公司、北京美科华仪科技有限公司、北京猎鹰安全科技有限公司、北京礼信年年餐饮管理有限公司、北京金山办公软件股份有限公司、北京金和网络股份有限公司、北京嘉业汇智科技发展有限公司、北京华宇软件股份有限公司、北京华电众信技术股份有限公司、北京宏景世纪软件股份有限公司、北京百卓网络技术有限公司、安元科技股份有限公司、安美世纪（北京）科技有限公司、安徽科迅教育装备集团有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心和 ONKYO 安桥安桥（上海）商贸有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司、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、中电科网络安全科技股份有限公司、中孚安全技术有限公司、贵州多彩网安科技有限公司、河南东方云盾信息技术有限公司、中资网络信息安全科技有限公司、江苏晟晖信息科技有限公司、联通数字科技有限公司、江苏锋刃信息科技有限公司、江苏极元信息技术有限公司、内蒙古中叶信息技术有限责任公司、快页信息技术有限公司、江西中和证信息安全技术有限公司、北京天防安全科技有限公司、北京微步在线科技有限公司、北京山石网科信息技术有限公司、西藏熙安信息技术有限责任公司、上海观安信息技术股份有限公司、成都安美勤信息技术股份有限公司、杭州默安科技有限公司、北京天下信安技术有限公司、北京时代新威信息技术有限公司、广西网信信息技术有限公司、成都愚安科技有限公司、联想集团、中国电力科学研究院有限公司-信息通讯研究所、北京卓识网安技术股份有限公司、北银金融科技有限责任公司、安徽天行网安信息安全技术有限公司、北京中关

村实验室、山石网科通信技术股份有限公司、辽宁海事局、河南灵创电子科技有限公司、深圳昂楷科技有限公司、山东云天安全技术有限公司及其他个人白帽子向 CNVD 提交了 11801 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）和上海交大向 CNVD 共享的白帽子报送的 9827 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）	6920	6920
深信服科技股份有限公司	2250	0
奇安信网神（补天平台）	2095	2095
新华三技术有限公司	1008	0
上海交大	812	812
北京神州绿盟科技有限公司	525	0
北京数字观星科技有限公司	385	0
安天科技集团股份有限公司	300	0
阿里云计算有限公司	162	0
恒安嘉新（北京）科技股份公司	108	0
北京启明星辰信息安全技术有限公司	85	9
北京天融信网络安全技术有限公司	79	1
北京知道创宇信息技术有限公司	69	0
杭州安恒信息技术股份有限公司	45	0
华为技术有限公司	33	0
北京升鑫网络科技有限公司（青藤云）	31	31
中国电信集团系统集成有限责任公司	20	1

北京长亭科技有限公司	17	3
北京安信天行科技有限公司	5	5
中国电信股份有限公司网络安全产品运营中心	4	4
远江盛邦（北京）网络安全科技股份有限公司	3	3
北京智游网安科技有限公司	3	3
江苏金盾检测技术股份有限公司	152	152
中电科网络安全科技股份有限公司	53	3
中孚安全技术有限公司	46	46
贵州多彩网安科技有限公司	32	32
河南东方云盾信息技术有限公司	11	11
中资网络信息安全科技有限公司	8	8
江苏晟晖信息科技有限公司	7	7
联通数字科技有限公司	7	7
江苏锋刃信息科技有限公司	6	6
江苏极元信息技术有限公司	5	5
内蒙古中叶信息技术有限责任公司	5	5
快页信息技术有限公	5	5

司		
江西中和证信息安全技术有限公司	5	5
北京天防安全科技有限公司	4	4
北京微步在线科技有限公司	4	4
北京山石网科信息技术有限公司	3	3
西藏熙安信息技术有限责任公司	3	3
上海观安信息技术股份有限公司	3	3
成都安美勤信息技术股份有限公司	3	3
杭州默安科技有限公司	2	2
北京天下信安技术有限公司	2	2
北京时代新威信息技术有限公司	2	2
广西网信信息技术有限公司	2	2
成都愚安科技有限公司	2	2
联想集团	2	2
西门子（中国）有限公司	1	0
中国电力科学研究院有限公司-信息通讯研究所	1	1
北京卓识网安技术股份有限公司	1	1
北银金融科技有限责任公司	1	1

安徽天行网安信息安全技术有限公司	1	1
北京中关村实验室	1	1
山石网科通信技术股份有限公司	1	1
辽宁海事局	1	1
河南灵创电子科技有限公司	1	1
深圳昂楷科技有限公司	1	1
山东云天安全技术有限公司	1	1
CNCERT 广西分中心	2	2
CNCERT 宁夏分中心	1	1
CNCERT 河北分中心	1	1
个人	1576	1576
报送总计	16924	11801

本周漏洞按类型和厂商统计

本周，CNVD 收录了 394 个漏洞。WEB 应用 204 个，应用程序 112 个，网络设备（交换机、路由器等网络端设备）45 个，操作系统 17 个，智能设备（物联网终端设备）11 个，安全产品 5。

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	204
应用程序	112
网络设备（交换机、路由器等网络端设备）	45
操作系统	17
智能设备（物联网终端设备）	11
安全产品	5

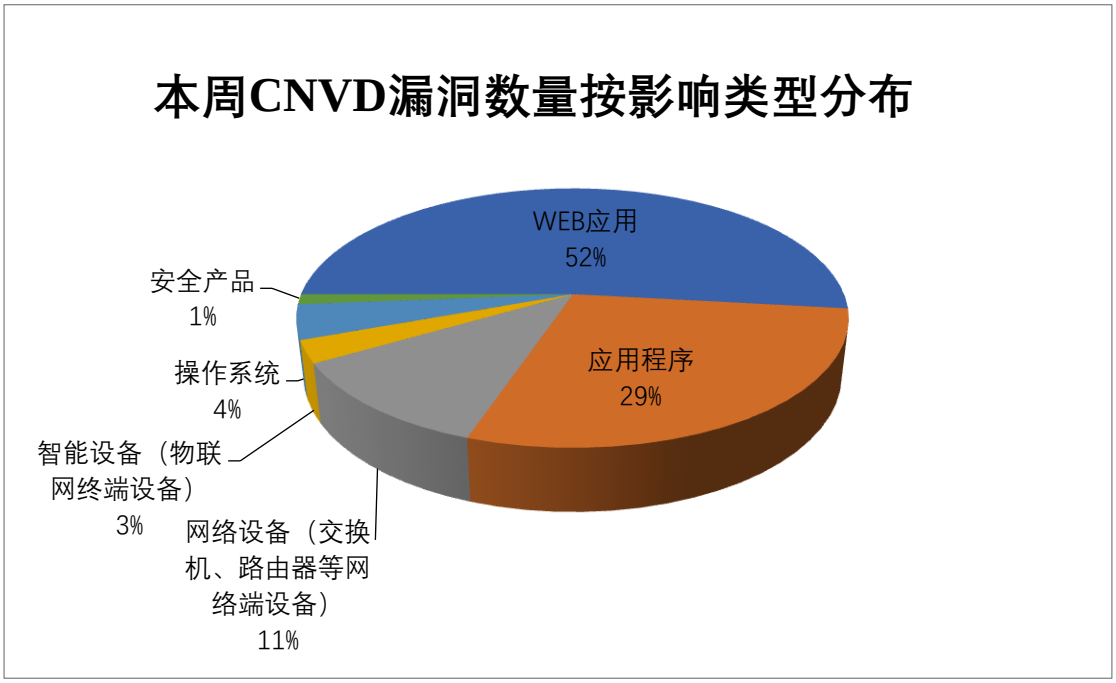

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、IBM、用友网络科技股份有限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	Adobe	23	6%
2	IBM	21	5%
3	用友网络科技股份有限公司	18	5%
4	北京星网锐捷网络技术有限公司	13	3%
5	Linux	11	3%
6	WordPress	11	3%
7	Mozilla	11	3%
8	中兴通讯股份有限公司	10	2%
9	Apache	8	2%
10	其他	268	68%

本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，39 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“TP-LINK ER7206 操作系统命令注入漏洞（CNVD-2024-15547）、Advantech WebAccess/SCADA 任意文件上传漏洞”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/

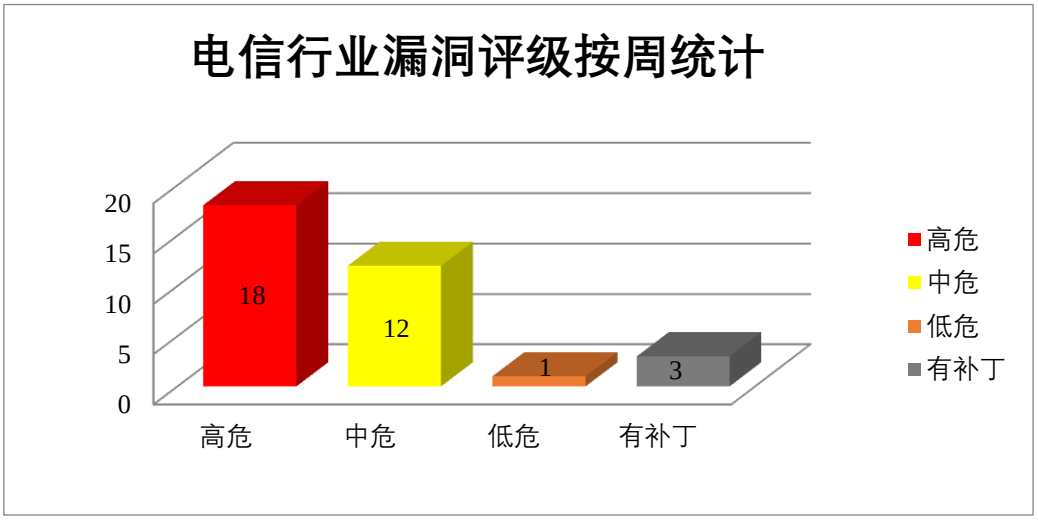

图 3 电信行业漏洞统计

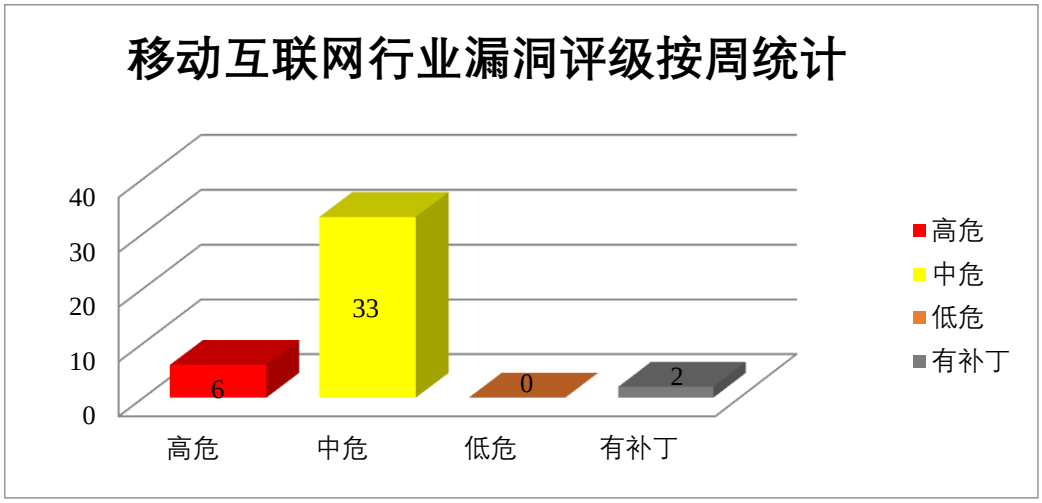

图 4 移动互联网行业漏洞统计

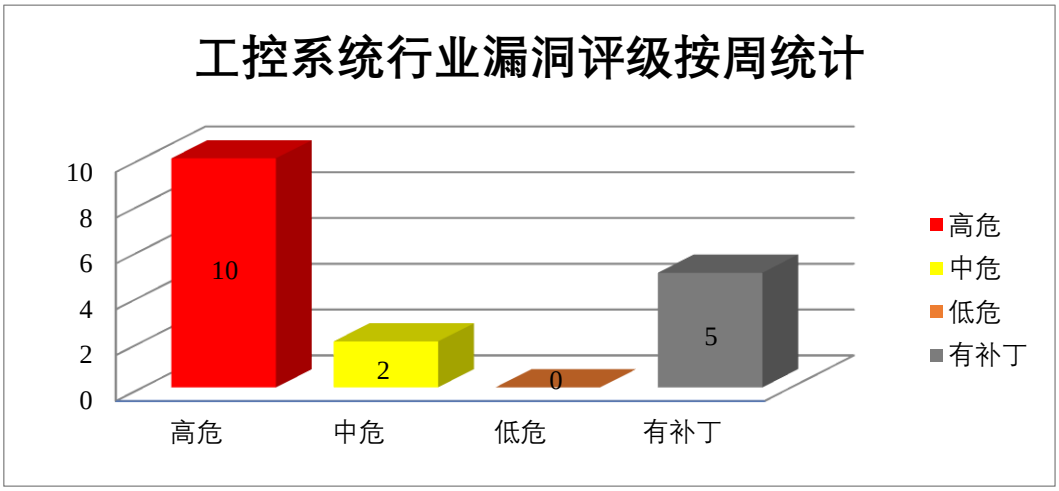

图 5 工控系统行业漏洞统计

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、 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，攻击者可利用漏洞将恶意脚本注入易受攻击的网页中。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-14654、CNVD-2024-14653、CNVD-2024-14657、CNVD-2024-14655、CNVD-2024-14661、CNVD-2024-14660、CNVD-2024-14659、CNVD-2024-14658）。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-2024-14654
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14653
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14657
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14655
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14661
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14660
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14659
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14658

2、 IBM 产品安全漏洞

IBM Integration Bus（IBM WebSphere Message Broker）是美国国际商业机器（IBM）公司的一款企业服务总线（ESB）产品。该产品为面向服务架构（SOA）环境和非 SOA 环境提供连通性和通用数据转换。IBM DS8900F HMC 是一款企业级磁盘存储系统，用于存储和管理大规模的企业数据。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。IBM i 是一套运行在 IBM Power Systems 和 IBM PureSystems 中的操作系统。IBM AIX 是一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过授权用户的身份验证限制，获取敏感信息或消耗内存资源，导致任意删除文件，任意命令执行等。

CNVD 收录的相关漏洞包括：IBM Integration Bus for z/OS 跨站请求伪造漏洞、IBM DS8900F HMC 信息泄露漏洞、IBM DS8900F HMC 授权问题漏洞、IBM DS8900F HMC 任意文件删除漏洞、IBM Maximo Asset Management XML 外部实体注入漏洞、

IBM DS8900F HMC 日志信息泄露漏洞、IBM i 权限许可和访问控制问题漏洞、IBM AIX/VIOS 命令执行漏洞。其中，除“IBM DS8900F HMC 信息泄露漏洞、IBM DS8900F HMC 授权问题漏洞、IBM DS8900F HMC 任意文件删除漏洞、IBM DS8900F HMC 日志信息泄露漏洞”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-2024-14666
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14671
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14670
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14669
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14667
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14672
https://www.cnvd.org.cn/flaw/show/CNVD-2024-15370
https://www.cnvd.org.cn/flaw/show/CNVD-2024-15371

3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致拒绝服务，本地权限提升，代码执行等。

CNVD 收录的相关漏洞包括：Linux kernel 代码问题漏洞（CNVD-2024-14763）、Linux kernel 资源管理错误漏洞（CNVD-2024-14762）、Linux kernel 代码执行漏洞（CNVD-2024-14767）、Linux Kernel 拒绝服务漏洞（CNVD-2024-14766、CNVD-2024-14768）、Linux Kernel 越界访问漏洞（CNVD-2024-14764）、Linux kernel 释放后使用漏洞（CNVD-2024-14772）、Linux kernel 竞争条件问题漏洞（CNVD-2024-14771）。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-2024-14763
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14762
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14767
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14766
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14764
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14768
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14772
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14771

4、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox（Web 浏

览器）的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞创建无效的 wasm 值，在系统上执行任意代码或导致拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox ESR 和 Thunderbird 拒绝服务漏洞、多款 Mozilla 产品代码执行漏洞（CNVD-2024-14974、CNVD-2024-14975、CNVD-2024-14977、CNVD-2024-14978、CNVD-2024-14979）、Mozilla Firefox 代码执行漏洞（CNVD-2024-14981）、Mozilla Firefox 安全绕过漏洞（CNVD-2024-14982）。其中，除“Mozilla Firefox 安全绕过漏洞（CNVD-2024-14982）”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-2024-14972
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14974
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14975
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14977
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14978
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14979
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14981
https://www.cnvd.org.cn/flaw/show/CNVD-2024-14982

5、Rockwell Automation PowerFlex 527 拒绝服务漏洞

Rockwell Automation PowerFlex 527 是美国罗克韦尔（Rockwell Automation）公司的一款可调交流变频器。本周，Rockwell Automation PowerFlex 527 被披露存在拒绝服务漏洞。攻击者可利用该漏洞导致设备崩溃。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-2024-15540

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-2024-14758	Apache Pulsar 访问控制错误漏洞（CNVD-2024-14758）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/ods5tq2hpl390hvjnvxv0bcg4rfpgjj8
CNVD-2024-14780	Hospital Management System SQL 注入漏洞（CNVD-2024-14780）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/kishan0725/Hospital-Management-System/issues/18

CNVD-2024-14974	多款 Mozilla 产品代码执行漏洞（CNVD-2024-14974）	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/mfsa2024-12/ https://www.mozilla.org/security/advisories/mfsa2024-13/ https://www.mozilla.org/security/advisories/mfsa2024-14/
CNVD-2024-14981	Mozilla Firefox 代码执行漏洞（CNVD-2024-14981）	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/mfsa2024-12/
CNVD-2024-15370	IBM i 权限许可和访问控制问题漏洞	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/7140499
CNVD-2024-15539	Rockwell Automation Arena Simulation Software 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://download.rockwellautomation.com/esd/download.aspx?downloadid=RAid1141475
CNVD-2024-15542	Advantech WebAccess/SCADA 任意文件覆盖漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.com/en/support/details/installation?id=1-MS9MJV
CNVD-2024-15541	Advantech WebAccess/SCADA 任意文件上传漏洞（CNVD-2024-15541）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.com/en/support/details/installation?id=1-MS9MJV
CNVD-2024-15544	Huawei HarmonyOS 和 EMUI 拒绝服务漏洞（CNVD-2024-15544）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://device.harmonyos.com/en/docs/security/update/security-bulletins-phones-202401-0000001799942565
CNVD-2024-15547	TP-LINK ER7206 操作系统命令注入漏洞（CNVD-2024-15547）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tp-link.com/us/support/download/er7206/v1/#Firmware

小结：本周，Adobe 产品被披露存在跨站脚本漏洞，攻击者可利用漏洞将恶意脚本注入易受攻击的网页中。此外，IBM、Linux、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过授权用户的身份验证限制，获取敏感信息或消耗内存资源，在系统上执行任意代码或导致拒绝服务，任意删除文件等。另外，Rockwell Automation PowerFlex 527 被披露存在拒绝服务漏洞。攻击者可利用漏洞导致设备崩溃。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、dzzoffice 跨站脚本漏洞（CNVD-2024-15545）

验证描述

dzzoffice 是美国大桌子（dzzoffice）公司的一个可提供在线协同办公套件功能的平台。该平台可为用于提供在线文档、表格、网盘、演示等功能。

dzzoffice 2.02.1 SC UTF8 版本存在跨站脚本漏洞，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://github.com/zyx0814/dzzoffice/issues/244

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-15545

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. 暗藏 11 年的 Linux 漏洞曝光，可用于伪造 SUDO 命令

研究人员发现，Linux 操作系统中的 util-linux 软件包 wall 命令中存在漏洞，该漏洞名为 WallEscape，被追踪为 CVE-2024-28085，黑客能够利用该漏洞窃取密码或更改剪贴板。

参考链接：https://www.bleepingcomputer.com/news/security/decade-old-linux-wall-bug-helps-make-fake-sudo-prompts-steal-passwords/

2. 谷歌修复了在 Pwn2Own 2024 上利用的 Chrome 零日漏洞

谷歌本周二修复了 Chrome 网络浏览器中的七个安全漏洞，其中包括在 Pwn2Own Vancouver 2024 黑客竞赛期间利用的两个零日漏洞。

参考链接：https://www.bleepingcomputer.com/news/security/google-fixes-chrome-zero-days-exploited-at-pwn2own-2024/

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