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 08 日-2024 年 01 月 14 日 **2024 年第 2 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 344 个，其中高危漏洞 141 个、中危漏洞 191 个、低危漏洞 12 个。漏洞平均分值为 6.49。本周收录的漏洞中，涉及 0day 漏洞 251 个（占 73%），其中互联网上出现“Library Management System SQL 注入漏洞（CNVD-2024-01189）、RPCMS 跨站脚本漏洞（CNVD-2024-01190）”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 4842 个，与上周（5215 个）环比减少 7%。

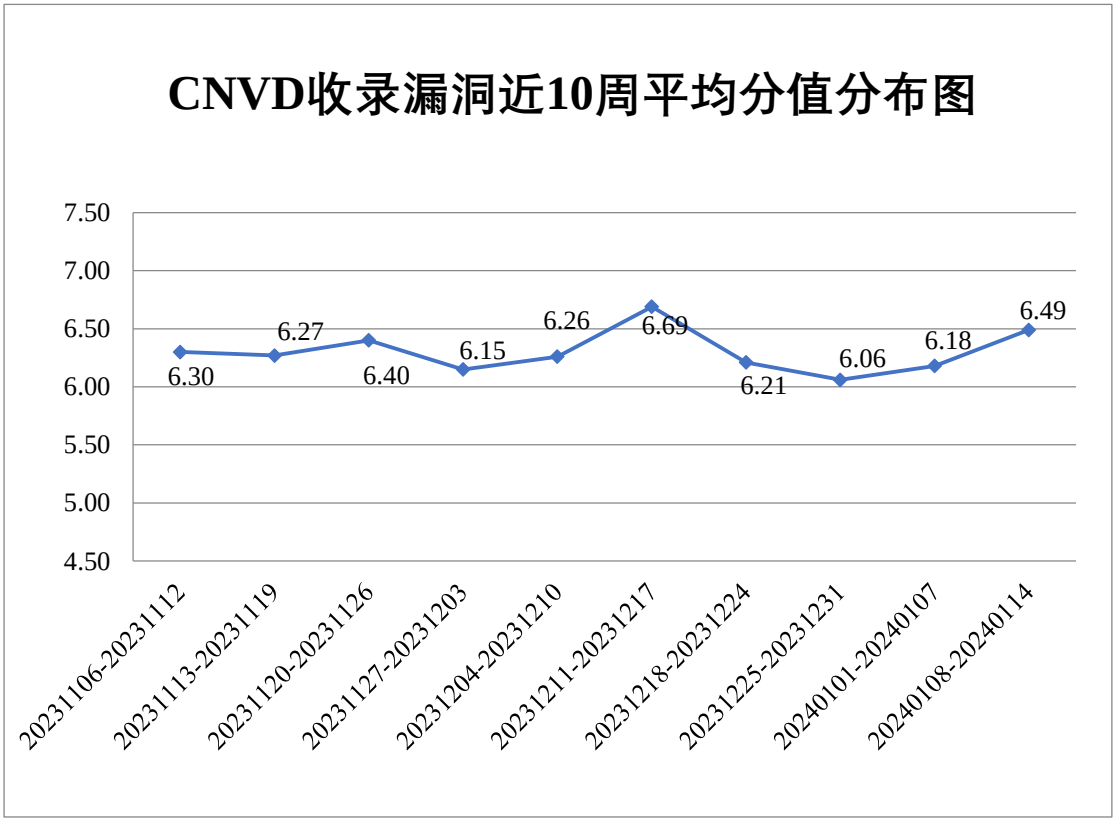

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 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 816 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 140 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 36 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：

卓豪（中国）技术有限公司、珠海派诺科技股份有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、重庆软狐信息技术有限公司、众勤通信设备贸易（上海）有限公司、中兴通讯股份有限公司、中国招标公共服务平台有限公司、智业软件股份有限公司、郑州一览科技有限公司、正奇晟业（北京）科技有限公司、浙江宇视科技有限公司、浙江联运知慧科技有限公司、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、云南链滴科技有限公司、云和恩墨（北京）信息技术有限公司、渔翁信息技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、小说精品屋、西安众邦网络科技有限公司、西安瑞友信息技术资讯有限公司、西安纳沃信息科技有限公司、西安旌旗电子股份有限公司、西安大西信息科技有限公司、武汉玖玖珈网络科技有限公司、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、统信软件技术有限公司、天津天视第六频道传媒有限责任公司、天津百望金赋科技有限公司、腾讯安全应急响应中心、宿州市涛盛网络科技有限公司、宿迁鑫潮信息技术有限公司、速达软件技术（广州）有限公司、苏州欧信达信息科技有限公司、苏州科达科技股份有限公司、四川众望升腾科技有限公司、四川东久科技股份有限公司、斯宝亚创（天津）电器有限公司广州分公司、世邦通信股份有限公司、深圳智慧光迅信息技术有限公司、深圳希施玛数据科技有限公司、深圳市思迅软件股份有限公司、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、深圳市金证优智科技有限公司、深圳市吉祥腾达科技有限公司、深圳市虹膜信息技术有限公司、深圳市好吃好喝网络技术有限公司、深圳市道尔智控科技股份有限公司、深圳昂楷科技有限公司、深信服科技股份有限公司、上海真兰仪表科技股份有限公司、上海栖闲科技工作室、上海普华科技发展股份有限公司、上海穆云智能科技有限公司、上海建业信息科技股份有限公司、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、上海观安信息技术股份有限公司、上海泛微网络科技股份有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、商丘芝麻开门网络科技有限公司、陕西华贝金服网络科技有限公司、山东卓文信息科技有限公司、山东中维世纪科技股份有限公司、山东运筹软件有限公司、山东科德电子有限公司、山东大众报业（集团）有限公司、厦

门天锐科技股份有限公司、厦门快普信息技术有限公司、厦门科拓通讯技术股份有限公司、厦门傲博教育科技有限公司、睿因科技（深圳）有限公司、融信世欧物业服务集团有限公司、曲靖蜂信科技有限公司、青岛恒泽水利科技有限公司、普联技术有限公司、南京科远智慧科技集团股份有限公司、纳龙健康科技股份有限公司、魔方动力、库课文化科技股份有限公司、京瓷（中国）商贸有限公司上海分公司、金蝶软件（中国）有限公司、金蝶国际软件集团有限公司、江苏捷成睿创科技发展有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华为技术有限公司、华平信息技术股份有限公司、华动泰越科技有限责任公司、湖南智尚科技发展有限公司、湖南汉坤实业有限公司、河北网星软件有限公司、杭州毓创科技有限公司、杭州与盟医疗技术有限公司、杭州逸曜信息技术有限公司、杭州雄伟科技开发股份有限公司、杭州西软信息技术有限公司、杭州合众数据技术有限公司、杭州浩腾智能科技开发有限公司、杭州海康威视系统技术有限公司、杭州恩软信息技术有限公司、杭州玳数科技有限公司、广州易达建信科技开发有限公司、广州信虹通信技术有限公司、广州全通数码科技有限公司、广州青鹿教育科技有限公司、广州璐华信息技术有限公司、广州华壹智能科技有限公司、广州红帆科技有限公司、广州白云区清泉宏知自学考试辅导中心有限责任公司、广联达科技股份有限公司、广东广凌信息科技股份有限公司、广东飞企互联科技股份有限公司、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、福州网钛软件科技有限公司、福建科立讯通信有限公司、福建博思软件股份有限公司、福建奥拓美科技有限公司、东莞市宇腾信息科技有限公司、东莞市通天星软件科技有限公司、鼎捷软件股份有限公司、电能易购（北京）科技有限公司、帝兴软件开发有限公司、大汉软件股份有限公司、成都元素科技有限公司、比亚迪股份有限公司、北京中科大洋科技发展股份有限公司、北京用友政务软件股份有限公司、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、北京鑫锐诚毅数字科技有限公司、北京新时空科技股份有限公司、北京五指互联科技有限公司、北京网康科技有限公司、北京万户网络技术有限公司、北京万户软件技术有限公司、北京世纪超星信息技术发展有限责任公司、北京深睿博联科技有限责任公司、北京人大金仓信息技术股份有限公司、北京龙软科技股份有限公司、北京金和网络股份有限公司、北京火木科技有限公司、北京慧图科技（集团）股份有限公司、北京华腾网讯科技有限公司、北京宏景世纪软件股份有限公司、北京瀚维特科技有限公司、北京海量数据技术股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、北京奥博威斯科技有限公司、安美世纪（北京）科技有限公司、安徽生命港湾信息技术有限公司、安徽青柿信息科技有限公司、DELTA_IABG 和 ABB。

本周，CNVD 发布了《Microsoft 发布 2024 年 1 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9636

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、新华三技术有限公司、北京启明星辰信息安全技术有限公司、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、河南东方云盾信息技术有限公司、江苏云天网络安全技术有限公司、西门子（中国）有限公司、联想集团、内蒙古洞明科技有限公司、贵州多彩网安科技有限公司、北京卓识网安技术股份有限公司、快页信息技术有限公司、亚信科技（成都）有限公司、中电科网络安全科技股份有限公司、湖南泛联新安信息科技有限公司、北京山石网科信息技术有限公司、安徽锋刃信息科技有限公司、苏州棱镜七彩信息科技有限公司、北京冠程科技有限公司、南京先维信息技术有限公司、西安秦易信息技术有限公司、安徽天行网安信息安全技术有限公司、杭州默安科技有限公司、星云博创科技有限公司、上海直画科技有限公司、江苏晟晖信息科技有限公司、任子行网络技术股份有限公司、含光实验室、江苏金陵科技集团有限公司、杭州弘沿科技有限公司、江苏极元信息技术有限公司、浙江木链物联网科技有限公司、中孚安全技术有限公司、广州安亿信软件科技有限公司、北京君云天下科技有限公司、南京深安科技有限公司、南京共美科技有限公司及其他个人白帽子向 CNVD 提交了 4842 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 3675 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）	1962	1962
斗象科技（漏洞盒子）	1146	1146
北京天融信网络安全技术有限公司	997	0
新华三技术有限公司	805	0
北京启明星辰信息安全技术有限公司	620	39
三六零数字安全科技集团有限公司	423	423
北京数字观星科技有限公司	314	0

安天科技集团股份有限公司	297	0
深信服科技股份有限公司	284	0
阿里云计算有限公司	209	0
天津市国瑞数码安全系统股份有限公司	187	0
上海交大	144	144
北京知道创宇信息技术有限公司	110	0
杭州安恒信息技术股份有限公司	95	14
中国电信集团系统集成有限责任公司	84	0
杭州迪普科技股份有限公司	7	0
北京安信天行科技有限公司	3	3
北京智游网安科技有限公司	2	2
西安四叶草信息技术有限公司	2	2
华为技术有限公司	1	1
北京神州绿盟科技有限公司	1	1
江苏金盾检测技术股份有限公司	108	108
河南东方云盾信息技术有限公司	36	36
江苏云天网络安全技术有限公司	23	23
西门子（中国）有限公司	21	0
联想集团	19	19
内蒙古洞明科技有限	15	15

公司		
贵州多彩网安科技有限公司	15	15
北京卓识网安技术股份有限公司	12	12
快页信息技术有限公司	11	11
亚信科技（成都）有限公司	10	10
中电科网络安全科技股份有限公司	8	8
湖南泛联新安信息科技有限公司	8	8
北京山石网科信息技术有限公司	7	7
安徽锋刃信息科技有限公司	7	7
苏州棱镜七彩信息科技有限公司	4	4
北京冠程科技有限公司	4	4
南京先维信息技术有限公司	4	4
西安秦易信息技术有限公司	4	4
安徽天行网安信息安全技术有限公司	3	3
杭州默安科技有限公司	3	3
星云博创科技有限公司	2	2
上海直画科技有限公司	2	2
江苏晟晖信息科技有限公司	2	2

任子行网络技术股份有限公司	2	2
含光实验室	1	1
江苏金陵科技集团有限公司	1	1
杭州弘沿科技有限公司	1	1
江苏极元信息技术有限公司	1	1
浙江木链物联网科技有限公司	1	1
中孚安全技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京君云天下科技有限公司	1	1
南京深安科技有限公司	1	1
南京共美科技有限公司	1	1
CNCERT 河北分中心	1	1
个人	785	785
报送总计	8819	4842

本周漏洞按类型和厂商统计

本周，CNVD 收录了 344 个漏洞。WEB 应用 153 个，应用程序 100 个，网络设备（交换机、路由器等网络端设备）42 个，智能设备（物联网终端设备）20 个，操作系统 19 个，安全产品 7 个，数据库 3 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	153
应用程序	100
网络设备（交换机、路由器等网络端设备）	42

智能设备（物联网终端设备）	20
操作系统	19
安全产品	7
数据库	3

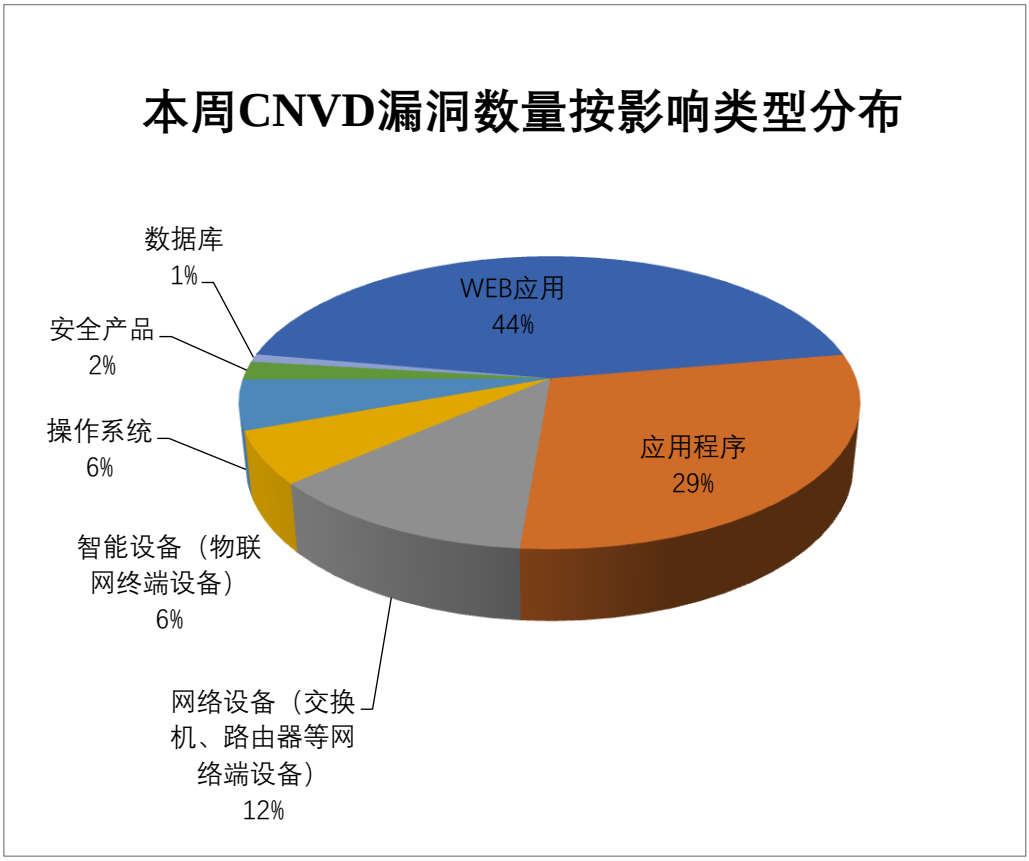

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SIEMENS、Apache、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	SIEMENS	21	6%
2	Apache	18	5%
3	Google	16	5%
4	Adobe	15	4%
5	IBM	9	3%
6	北京星网锐捷网络技术有限公司	9	3%
7	广州图创计算机软件开发有限公司	7	2%
8	佳能（中国）有限公司	7	2%
9	FFmpeg	7	2%
10	其他	235	68%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，29 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Siemens CPCI85 Firmware of SICAM A8000 Devices 命令注入漏洞、TP-LINK TL-ER5120G 命令执行漏洞”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/

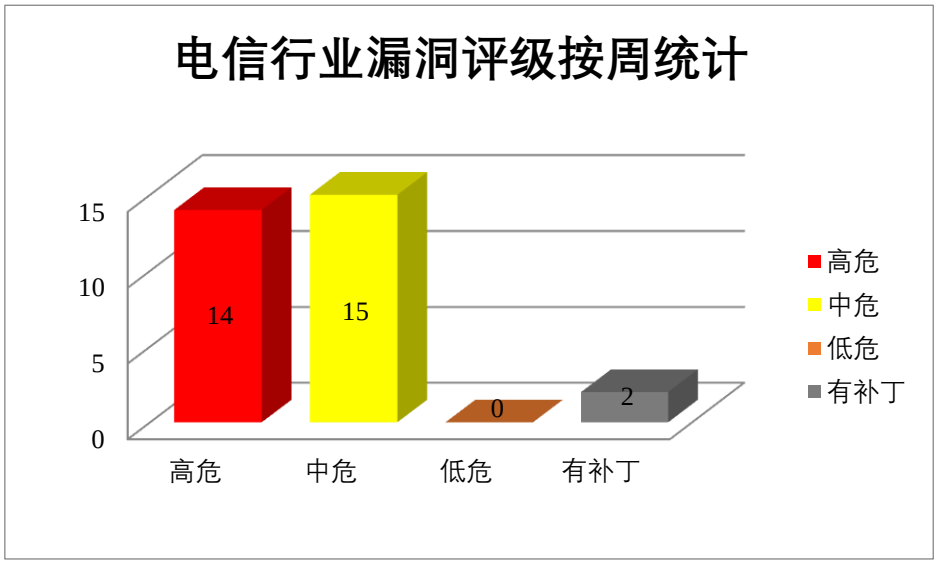

图 3 电信行业漏洞统计

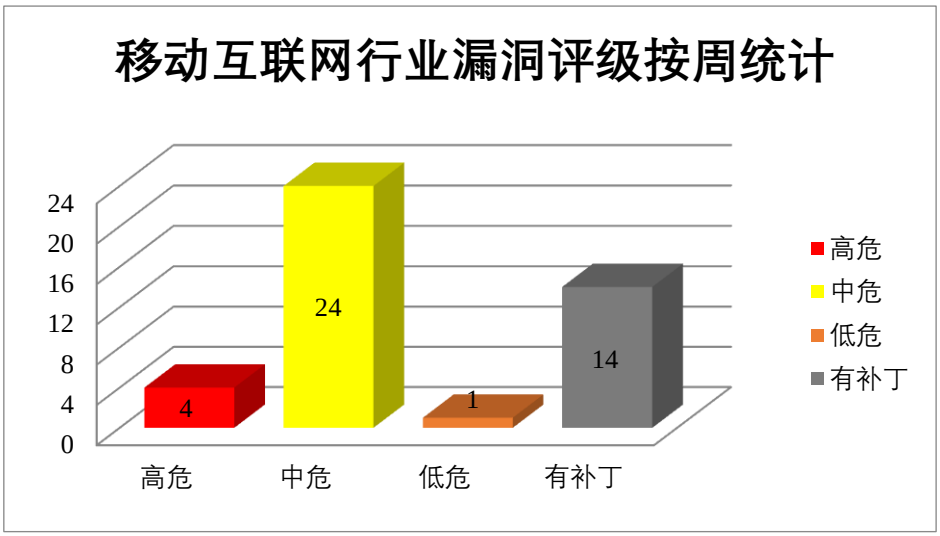

图 4 移动互联网行业漏洞统计

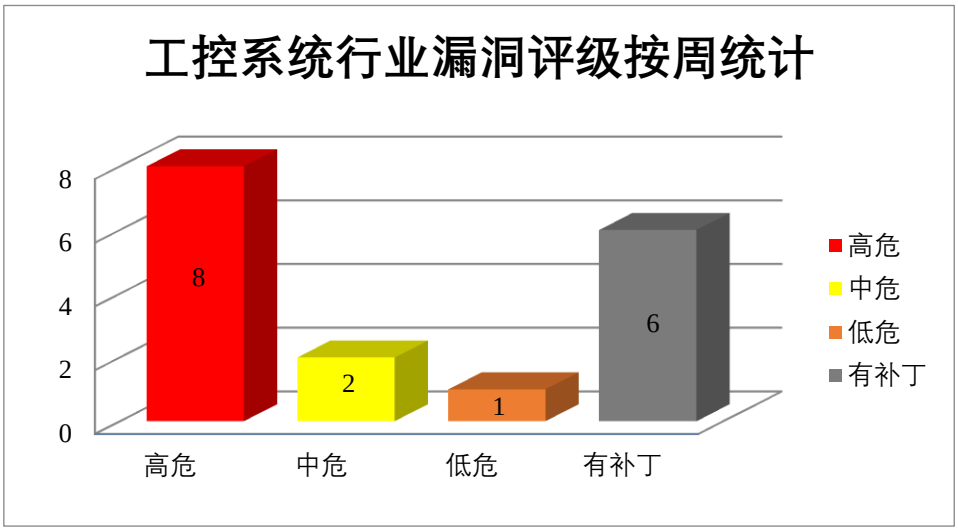

图 5 工控系统行业漏洞统计

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、 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，在系统上获得更高的权限。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2024-01353、CNVD-2024-01354、CNVD-2024-01355、CNVD-2024-01356、CNVD-2024-01368、CNVD-2024-01369、CNVD-2024-01377）、Google Android 权限提升漏洞（CNVD-2024-01363）。其中，“Google Android 权限提升漏洞（CNVD-2024-01363）、Google Android 信息泄露漏洞（CNVD-2024-01377）”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-2024-01353

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01354

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01355

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01356

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01363

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01368

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01369

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01377

2、 IBM 产品安全漏洞

IBM Planning Analytics 是美国国际商业机器（IBM）公司的一套业务规划分析解决方案。该方案支持自动化执行业务规划、预算和分析等流程。IBM AIX 是美国国际商业机器（IBM）公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM Rational Asset Manager 是美国 IBM 公司的一种协作软件开发工具。组织可以使用它来识别、管理和治理软件资产和服务的设计、开发和使用。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 QRadar SIEM 是美国国际商业机器（IBM）公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。IBM Security Verify Access（ISAM）是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM TRIRIGA Application Platform 是美国国际商业机器（IBM）公司的一套用于部署 TRIRIGA 应用的技术平台。该平台提供了一组设计时和运行时组件，分别用于构建和运行其企业级应用，并支持客户特定的配置，而无需更改源代码。IBM Tivoli Workload Scheduler 是美国国际商业机器（IBM）公司的一套企业任务调度软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发送特制的 HTTP 请求上传恶意脚本，从而导致在易受攻击的系统上执行任意代码，导致拒绝服务攻击，执行远程代码等。

CNVD 收录的相关漏洞包括：IBM Planning Analytics 代码问题漏洞（CNVD-2024-01168）、IBM AIX 输入验证错误漏洞（CNVD-2024-01169）、IBM Rational Asset Manager 权限控制问题漏洞、IBM i 授权问题漏洞、IBM QRadar SIEM 跨站脚本漏洞（CNVD-2024-01173）、IBM Security Verify Access 资源管理错误漏洞、IBM TRIRIGA Application Platform 跨站脚本漏洞（CNVD-2024-01175）、IBM Tivoli Workload Scheduler XML 外部实体注入漏洞。其中，“IBM Planning Analytics 代码问题漏洞（CNVD-2024-01168）、IBM Security Verify Access 资源管理错误漏洞、IBM Tivoli Workload Scheduler XML 外部实体注入漏洞”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-2024-01168
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01169
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01170
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01172
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01173
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01174
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01175

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01176

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-2024-01177、CNVD-2024-01178、CNVD-2024-01179、CNVD-2024-01180、CNVD-2024-01181、CNVD-2024-01182、CNVD-2024-01183、CNVD-2024-01184）。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-2024-01177

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01178

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01179

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01180

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01181

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01182

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01183

https://www.cnvd.org.cn/flaw/show/CNVD-2024-01184

4、Apache 产品安全漏洞

Apache OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache Guacamole 是美国阿帕奇（Apache）基金会的一款无客户端的远程桌面网关。该产品支持 VNC、RDP 和 SSH 等协议。Apache Pulsar 是美国阿帕奇（Apache）基金会的一个用于云环境种，集消息、存储、轻量化函数式计算为一体的分布式消息流平台。Apache IoTDB 是美国阿帕奇（Apache）基金会的一款为时间序列数据设计的集成数据管理引擎，它能够提供数据收集、存储和分析服务等。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 Dubbo 是美国阿帕奇（Apache）基金会的一款基于 Java 的轻量级 RPC（远程过程调用）框架。该产品提供了基于接口的远程呼叫、容错和负载平衡以及自动服务注册和发现等功能。Apache Doris 是美国阿帕奇（Apache）基金会的一个现代 MPP 分析数据库产品。可以提供亚秒级查询和高效的实时数据分析。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发送特制请求进行 SSRF 攻击，读取任意文件属性，导致拒绝服务，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Apache OFBiz 服务器端请求伪造漏洞、Apache OF

Biz 服务器端请求伪造漏洞（CNVD-2024-01013）、Apache Guacamole 整数溢出漏洞、Apache Pulsar WebSocket Proxy 拒绝服务漏洞、Apache IoTDB 反序列化漏洞、Apache Airflow 跨站请求伪造漏洞（CNVD-2024-01017）、Apache Dubbo 代码问题漏洞（CNVD-2024-02173）、Apache Doris 授权问题漏洞。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-2024-01012
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01013
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01020
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01019
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01018
https://www.cnvd.org.cn/flaw/show/CNVD-2024-01017
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02173
https://www.cnvd.org.cn/flaw/show/CNVD-2024-02172

5、TP-LINK Tapo C100 拒绝服务漏洞

TP-LINK Tapo C100 是中国普联（TP-LINK）公司的一款网络摄像头设备。本周，TP-LINK Tapo C100 被披露存在拒绝服务漏洞。攻击者可利用该漏洞通过提供精心设计的 Web 请求来导致拒绝服务(DoS)。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-2024-02155

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-2024-01391	Siemens JT2Go 和 Teamcenter Visualization 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://cert-portal.siemens.com/productcert/html/ssa-794653.html
CNVD-2024-01390	Siemens JT2Go 和 Teamcenter Visualization 缓冲区溢出漏洞（CNVD-2024-01390）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-794653.html
CNVD-2024-01398	maxView Storage Manager 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-702935.html
CNVD-2024	PrestaShop SQL 注入漏洞（C	高	厂商已发布了漏洞修复程序，请及

-02171	NVD-2024-02171）		时关注更新：https://security.friendsofpresta.org/modules/2023/12/19/baproductzoommagnifier.html
CNVD-2024-02175	MajorDoMo 命令执行漏洞（CNVD-2024-02175）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/sergejey/majordomo/commit/0662e5ebfb133445ff6154b69c61019357092178
CNVD-2024-01396	Siemens SIMATIC CN 4100 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-777015.html
CNVD-2024-01395	Siemens SIMATIC CN 4100 使用默认凭证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-777015.html
CNVD-2024-01393	Siemens JT2Go 和 Teamcenter Visualization 越界读取漏洞（CNVD-2024-01393）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-794653.html
CNVD-2024-01399	Siemens Solid Edge 未初始化指针访问漏洞（CNVD-2024-01399）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-589891.html
CNVD-2024-01397	Siemens SIMATIC CN 4100 授权绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-777015.html

小结：本周，Google 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，在系统上获得更高的权限。此外，IBM、Adobe、Apache 等多款产品被披露存在多个漏洞，攻击者可利用漏洞发送特制的 HTTP 请求上传恶意脚本，从而导致在易受攻击的系统上执行任意代码，导致拒绝服务攻击，执行远程代码等。另外，TP-LINK Tapo C100 被披露存在拒绝服务漏洞。攻击者可利用漏洞通过提供精心设计的 Web 请求来导致拒绝服务(DoS)。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、Library Management System SQL 注入漏洞（CNVD-2024-01189）

验证描述

Library Management System 是一个带有二维码考勤和自动生成借书证的图书馆管理系统。

Library Management System v2.0 版本存在 SQL 注入漏洞，该漏洞源于 index.php 中的参数 category 缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/h4md153v63n/CVEs/blob/main/Library-Management-System/Library-Management-System_SQL_Injection-3.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-01189

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. T-Mobile 又出网络故障，导致账户访问和移动应用程序瘫痪

T-Mobile 近期又发生重大网络故障，导致其用户无法登录账户和使用该公司的移动应用程序。

参考链接：https://www.bleepingcomputer.com/news/technology/major-t-mobile-outage-takes-down-account-access-mobile-app/

2. 超过 15 万个 WordPress 网站面临被漏洞插件接管的风险

POST SMTP Mailer WordPress 插件是一种电子邮件发送工具，有 30 万个网站在使用，其中的两个漏洞可能会帮助攻击者完全控制网站验证。

参考链接：https://www.bleepingcomputer.com/news/security/over-150k-wordpress-sites-at-takeover-risk-via-vulnerable-plugin/

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