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 10 日-2024 年 06 月 16 日 **2024 年第 24 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 333 个，其中高危漏洞 178 个、中危漏洞 145 个、低危漏洞 10 个。漏洞平均分值为 6.74。本周收录的漏洞中，涉及 0day 漏洞 259 个（占 78%），其中互联网上出现“JFinalCMS 跨站脚本漏洞（CNVD-2024-26516）、MiniCMS 跨站脚本漏洞（CNVD-2024-24950）”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 4795 个，与上周（2293 个）环比增多 1.09 倍。

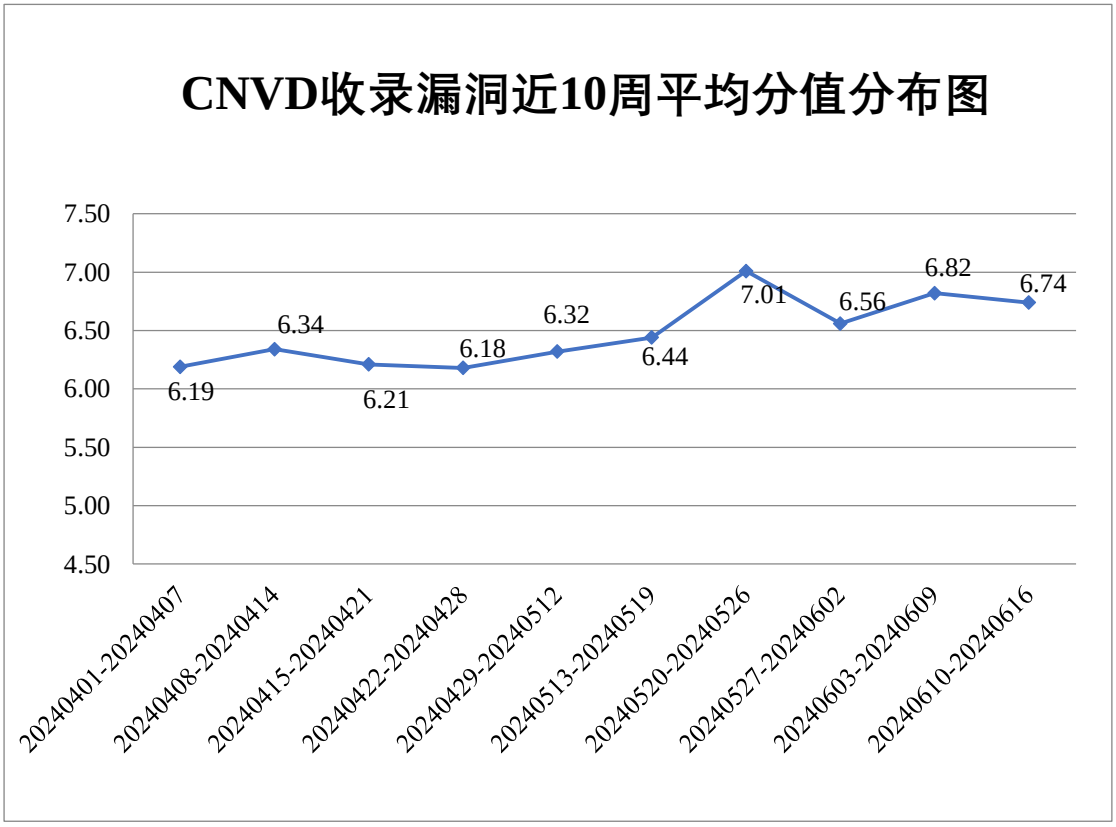

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 361 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 92 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 17 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、中网智达（河北）网络科技有限公司、智互联（深圳）科技有限公司、浙江华锐捷技术有限公司、浙江和达科技股份有限公司、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、英中传媒、武汉合智数字能源技术有限公司、无锡信捷电气股份有限公司、统信软件技术有限公司、天津市匠人匠心科技有限公司、唐山市柳林自动化设备有限公司、太原宏远智诚科技有限公司、索尼（中国）有限公司、苏州万户网络科技有限公司、苏州空谷网络科技有限公司、苏州科达科技股份有限公司、苏州华企立方信息技术有限公司、四川掌上时代科技有限公司、深圳市中电数通智慧安全科技股份有限公司、深圳市月歌科技有限公司、深圳市旺龙智能科技有限公司、深圳市荣宇翔科技有限公司、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、深圳市博实结科技股份有限公司、深圳警翼智能科技股份有限公司、深圳方维网络科技有限公司、深圳达实物联网技术有限公司、深圳创维数字技术有限公司、深圳奥联信息安全技术有限公司、申瓯通信设备有限公司、绍兴智合信息技术有限公司、上海卓卓网络科技有限公司、上海雍熙信息技术有限公司、上海桑锐电子科技股份有限公司、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、上海百胜软件股份有限公司、上海百奇网络信息技术有限公司、山石网科通信技术（北京）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、厦门得推网络科技有限公司、三一网络技术有限公司、三未信安科技股份有限公司、若依、融智通信息科技（天津）有限公司、青岛中翔汇智网络科技有限公司、青岛海信网络科技股份有限公司、麒麟软件有限公司、利盟信息技术（中国）有限公司、佳能（中国）有限公司、济南亘安信息技术有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖北展邦信息技术有限公司、宏脉信息技术（广州）股份有限公司、河南华企祥云计算机科技有限公司、合肥捷助医药科技有限公司、杭州雄伟科技开发股份有限公司、杭州新中大科技股份有限公司、杭州可道云网络有限公司、杭州海康威视数字技术股份有限公司、海南宸芯科技有限公司、贵阳思普信息技术有限公司、广州同鑫科技有限公司、广州睿狐科技有限公司、广州联浩网络科技有限公司、广联达科技股份有限公司、广东米可信息技术有限公司、广东好快省汽车服务有限公司、富士施乐（中国）有限公司、佛山市推搜网络科技有限公司、东莞市恒点互联科技有限公司、郸城县

新翔软件科技有限公司、成都长益西联软件有限公司、成都猴子软件有限公司、畅捷通信息技术股份有限公司、北京中盛普阳科技发展有限公司、北京亿赛通科技发展有限责任公司、北京一采通信息科技有限公司、北京兴辅科技有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京万户网络技术有限公司、北京通达信科科技有限公司、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、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京爱国小男孩科技有限公司、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、安徽八度网络科技有限公司、爱普生（中国）有限公司和 MindSpore 开源社区。

本周，CNVD 发布了《Microsoft 发布 2024 年 6 月安全更新》，详情参见 CNVD 网站公告内容（https://www.cnvd.org.cn/webinfo/show/10111）。

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、北京启明星辰信息安全技术有限公司、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。快页信息技术有限公司、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、马鞍山书拓安全科技有限公司、成都久信信息技术股份有限公司、中孚安全技术有限公司、北京中睿天下信息技术有限公司、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、北京天下信安技术有限公司、北京翰慧投资咨询有限公司、苏州棱镜七彩信息科技有限公司、华信咨询设计研究院有限公司、厦门聚丁科技有限公司、联通数字科技有限公司、南方电网数字电网集团信息通信科技有限公司、上海直画科技有限公司、中资网络信息安全科技有限公司、润成安全技术有限公司、湖南泛联新安信息科技有限公司、江苏云天网络安全技术有限公司及其他个人白帽子向 CNVD 提交了 4795 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）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 4041 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）	2821	2821
天津市国瑞数码安全系统股份有限公司	1968	0
新华三技术有限公司	831	0
北京启明星辰信息安	732	3

全技术有限公司		
安天科技集团股份有限公司	599	0
三六零数字安全科技集团有限公司	495	495
奇安信网神（补天平台）	376	376
上海交大	349	349
北京数字观星科技有限公司	258	0
阿里云计算有限公司	144	0
北京天融信网络安全技术有限公司	120	5
恒安嘉新（北京）科技股份公司	86	0
华为技术有限公司	81	1
远江盛邦（北京）网络安全科技股份有限公司	60	60
北京长亭科技有限公司	44	1
北京知道创宇信息技术有限公司	42	0
中国电信股份有限公司网络安全产品运营中心	37	37
杭州安恒信息技术股份有限公司	17	8
北京安信天行科技有限公司	14	14
北京升鑫网络科技有限公司（青藤云）	13	13
杭州迪普科技股份有限公司	9	1
深信服科技股份有限	2	2

公司		
北京神州绿盟科技有限公司	1	1
快页信息技术有限公司	49	49
河南东方云盾信息技术有限公司	23	23
江苏金盾检测技术股份有限公司	17	17
西门子（中国）有限公司	14	0
马鞍山书拓安全科技有限公司	8	8
成都久信信息技术股份有限公司	7	7
中孚安全技术有限公司	6	6
北京中睿天下信息技术有限公司	5	5
安徽天行网安信息安全技术有限公司	3	3
中国电信股份有限公司上海研究院	2	2
北京天下信安技术有限公司	2	2
北京翰慧投资咨询有限公司	2	2
苏州棱镜七彩信息科技有限公司	2	2
华信咨询设计研究院有限公司	1	1
厦门聚丁科技有限公司	1	1
联通数字科技有限公司	1	1

南方电网数字电网集团信息通信科技有限公司	1	1
上海直画科技有限公司	1	1
中资网络信息安全科技有限公司	1	1
润成安全技术有限公司	1	1
湖南泛联新安信息科技有限公司	1	1
江苏云天网络安全技术有限公司	1	1
CNCERT 河北分中心	1	1
个人	472	472
报送总计	9721	4795

本周漏洞按类型和厂商统计

本周，CNVD 收录了 333 个漏洞。按类型划分包括 WEB 应用 186 个，应用程序 78 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）13 个，操作系统 10 个，安全产品 4。

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	186
应用程序	78
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）	13
操作系统	10
安全产品	4

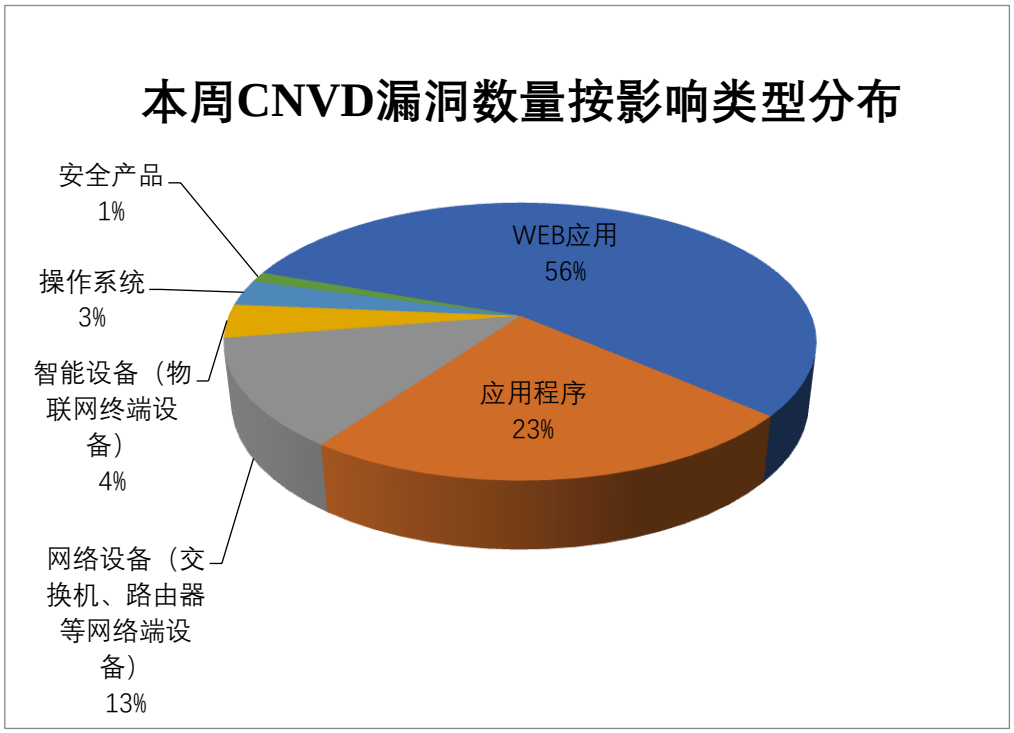

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WBSAirback、Apache、Siemens 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	WBSAirback	16	5%
2	Apache	14	4%
3	Siemens	14	4%
4	Google	10	3%
5	IBM	9	3%
6	Fortinet	7	2%
7	北京神州视翰科技有限公司	7	2%
8	北京百卓网络技术有限公司	7	2%
9	北京神州视翰科技有限公司	7	2%
10	其他	242	73%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，5 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“Siemens SINEC Traffic Analyzer 输入验证错误漏洞、

Siemens SINEC Traffic Analyzer 会话过期不足漏洞”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/

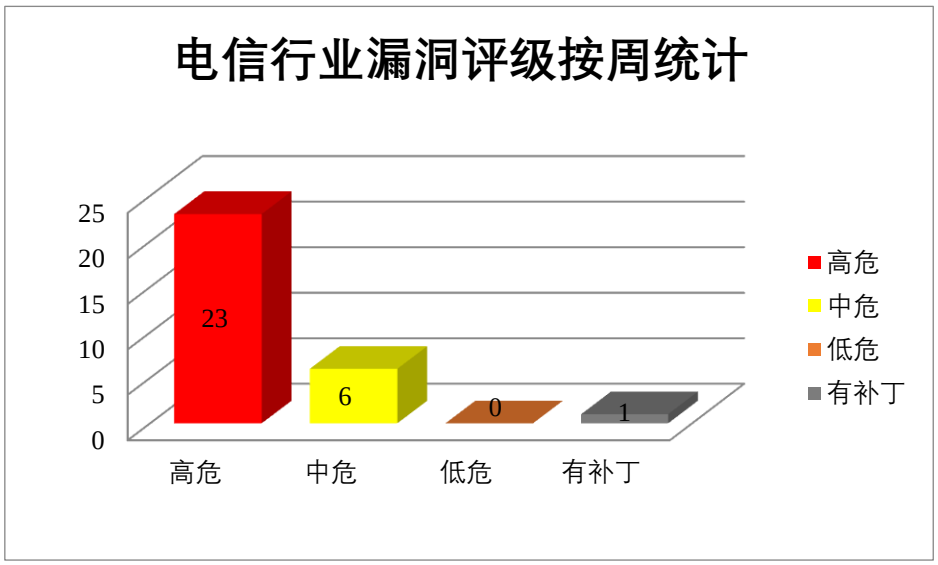

图 3 电信行业漏洞统计

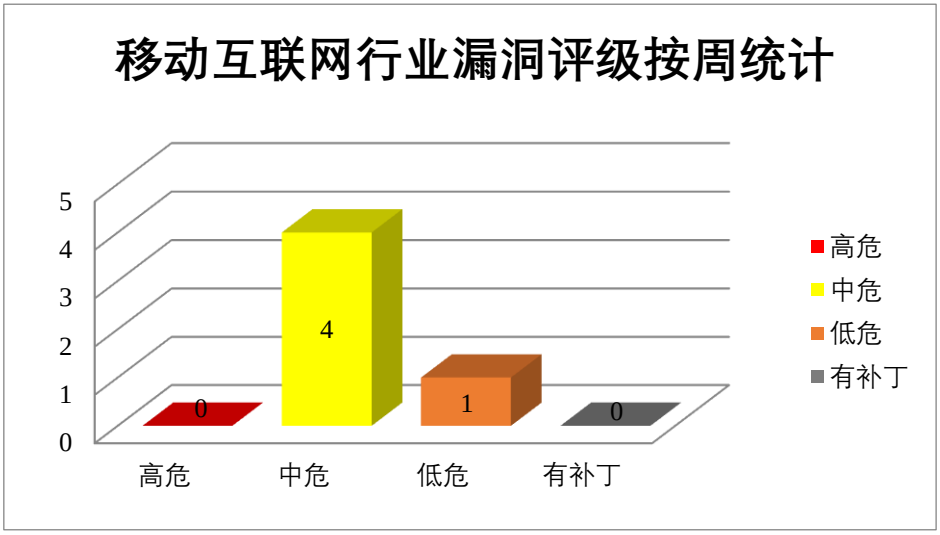

图 4 移动互联网行业漏洞统计

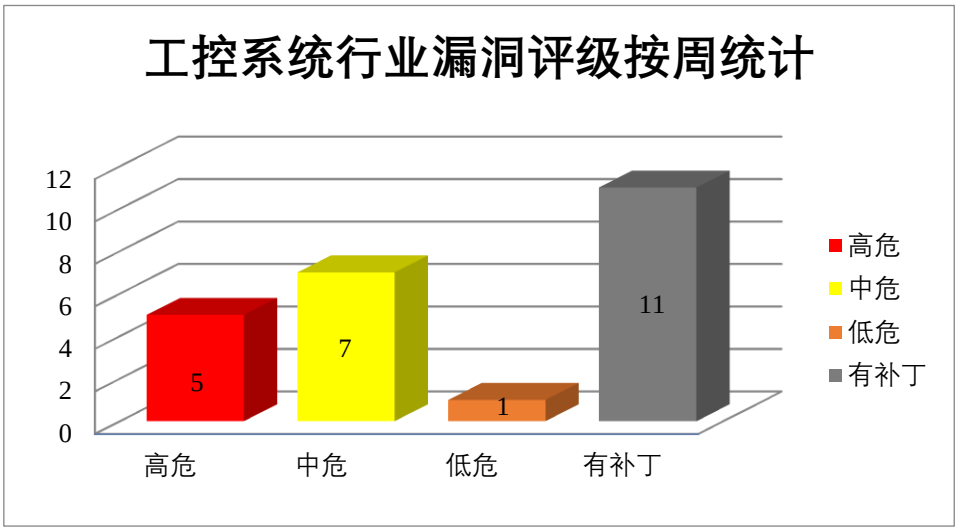

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM UrbanCode Deploy（UCD）是美国国际商业机器（IBM）公司的一套应用自动化部署工具。该工具基于一个应用部署自动化管理信息模型，并通过远程代理技术，实现对复杂应用在不同环境下的自动化部署等。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 Security Guardium 是美国国际商业机器（IBM）公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。IBM Aspera 是美国国际商业机器（IBM）公司的一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。IBM WebSphere Automation 是美国国际商业机器（IBM）公司的一个运营平台。自动化运营活动以主动降低安全风险并加速威胁修复。本周，上述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，在系统上执行任意命令等。

CNVD 收录的相关漏洞包括：IBM UrbanCode Deploy 跨站脚本漏洞（CNVD-2024-26496）、IBM Planning Analytics 跨站脚本漏洞（CNVD-2024-26495）、IBM Planning Analytics Local 跨站脚本漏洞（CNVD-2024-26494、CNVD-2024-26493）、IBM Security Guardium 操作系统命令注入漏洞（CNVD-2024-26499）、IBM Security Guardium 跨站脚本漏洞（CNVD-2024-26498）、IBM Aspera 跨站脚本漏洞（CNVD-2024-26497）、IBM WebSphere Automation 命令执行漏洞。其中，“IBM Security Guardium 操作系统命令注入漏洞（CNVD-2024-26499）”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-2024-26496

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26495

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26494

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26493

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26499

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26498

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26497

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26500

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代码执行漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面在沙箱内执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 代码执行漏洞（CNVD-2024-26520、CNVD-2024-26519、CNVD-2024-26522、CNVD-2024-26521、CNVD-2024-26524、CNVD-2024-26523、CNVD-2024-26527、CNVD-2024-26526）。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-2024-26520

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26519

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26522

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26521

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26524

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26523

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26527

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26526

3、 Apache 产品安全漏洞

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 Superset 是美国阿帕奇（Apache）基金会的一个数据可视化和数据探索平台。Apache Kafka 是美国阿帕奇（Apache）基金会的一套开源的分布式流媒体平台。该平台能够获取实时数据，用于构建对数据流的变化进行实时反应的应用程序。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，造成拒绝服务，通过发送精心编制的 SQL 语句，从而查看、添加、修改或删除后端数据库中的信息等。

CNVD 收录的相关漏洞包括：Apache Airflow 跨站脚本漏洞（CNVD-2024-26529）、

Apache Airflow 信息泄露漏洞（CNVD-2024-26530、CNVD-2024-26532、CNVD-2024-26539）、Apache Superset SQL 注入漏洞（CNVD-2024-26534、CNVD-2024-26537）、Apache Superset 信息泄露漏洞（CNVD-2024-26535）、Apache Kafka 拒绝拒绝漏洞。其中，“Apache Kafka 拒绝拒绝漏洞”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-2024-26529
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26530
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26532
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26534
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26535
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26537
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26539
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26543

4、Siemens 产品安全漏洞

TIM 1531 IRC 是 SIMATIC S7-1500, S7-400, S7-300 的通信模块。Mendix 是一个高生产力的应用程序平台，能够大规模构建和持续改进移动和 web 应用程序。SINEC Traffic Analyzer 是一个内部部署的应用程序，监控控制器和 IO 设备之间的 PNIO (PROFINET IO)通信。该软件检测 PROFINET 通信问题，并通过 Web-UI 向用户报告。PowerSys 是一个服务程序，用于 PowerLink 50/100 或 SWT 3000 设备的调试、维护和诊断。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，修改未经授权的文件，绕过身份验证，获取受管理远程设备的管理权限。

CNVD 收录的相关漏洞包括：Siemens TIM 1531 IRC 数字类型错误转换漏洞、Siemens Mendix 权限管理错误漏洞、Siemens SINEC Traffic Analyzer 逻辑缺陷漏洞、Siemens SINEC Traffic Analyzer 输入验证错误漏洞、Siemens SINEC Traffic Analyzer 跨站请求伪造漏洞、Siemens SINEC Traffic Analyzer 暴露的危险方法或功能漏洞、Siemens SINEC Traffic Analyzer 敏感信息明文传输漏洞、Siemens PowerSys 认证错误漏洞。其中“Siemens SINEC Traffic Analyzer 输入验证错误漏洞、Siemens SINEC Traffic Analyzer 跨站请求伪造漏洞、Siemens SINEC Traffic Analyzer 暴露的危险方法或功能漏洞、Siemens PowerSys 认证错误漏洞”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-2024-26692
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26690
https://www.cnvd.org.cn/flaw/show/CNVD-2024-26696

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26695

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26700

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26698

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26697

https://www.cnvd.org.cn/flaw/show/CNVD-2024-26702

5、WBSAirback 命令注入漏洞

WBSAirback 是 WBSAirback 公司的一个新一代存储和备份系统。本周，WBSAirback 被披露存在命令注入漏洞。攻击者可利用该漏洞修改预期命令。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-2024-27130

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-2024-26503	Fortinet FortiPortal 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-24-021
CNVD-2024-26508	Fortinet FortiWeb 资源管理错误漏洞（CNVD-2024-26508）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/advisory/FG-IR-21-138
CNVD-2024-26507	Fortinet FortiSOAR 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://docs.fortinet.com/document/fortisoar/7.2.1/getting-started-with-deploying-fortisoar
CNVD-2024-26525	Google Chrome 缓冲区溢出漏洞（CNVD-2024-26525）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_30.html
CNVD-2024-26528	Google Chrome 缓冲区溢出漏洞（CNVD-2024-26528）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_21.html
CNVD-2024-26533	Apache OFBiz 路径遍历漏洞（CNVD-2024-26533）	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/w6s60o

			kgkxp2th1sr8vx0ndmgk68fqrd
CNVD-2024-26689	Siemens Tecnomatix Plant Simulation 类型转换错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.sw.siemens.com/en-US/product/297028302/
CNVD-2024-27171	SolarWinds Serv-U FTP Server 目录遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28995
CNVD-2024-26501	IBM Cognos Analytics 存在未明漏洞（CNVD-2024-26501）	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/7149874
CNVD-2024-26701	Siemens SINEC Traffic Analyzer 会话过期不足漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.industry.siemens.com/cs/ww/en/view/109954887/

小结：本周，IBM 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，在系统上执行任意命令等。此外，Google、Apache、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面在沙箱内执行任意代码，获取敏感信息，造成拒绝服务，通过发送精心编制的 SQL 语句，从而查看、添加、修改或删除后端数据库中的信息等。另外，WBSAirback 被披露存在命令注入漏洞。攻击者可利用漏洞修改预期命令。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-2024-26516）

验证描述

JFinalCMS 是一个内容管理系统。

JFinalCMS 20221020 及之前版本存在跨站脚本漏洞，该漏洞源于文件/admin/content 的参数 Title 对用户提供的数据缺乏有效过滤与转义，攻击者利用该漏洞可以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://gitee.com/heyewei/JFinalcms/issues/I8VHM2

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-26516

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. 日本 2023 财年发生超 1.3 万件个人信息泄露事件

日本个人信息保护委员会 11 日发布报告称，2023 财年日本发生 13279 件个人信息泄露事件，是上一财年的 1.7 倍，为历史最多。

参考链接：https://baijiahao.baidu.com/s?id=1801522995973530231&wfr=spider&for=pc

2. 出于安全考虑，微软推迟了 Copilot+PC 的 AI 召回功能

Microsoft 透露，它推迟了有争议的人工智能（AI）驱动的 Copilot+PC 召回功能的推出，该功能之前被广泛认为存在隐私和安全风险。

参考链接：https://thehackernews.com/2024/06/microsoft-delays-ai-powered-recall.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