国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 05 月 13 日-2024 年 05 月 19 日 **2024 年第 20 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 696 个，其中高危漏洞 320 个、中危漏洞 351 个、低危漏洞 25 个。漏洞平均分值为 6.44。本周收录的漏洞中，涉及 0day 漏洞 592 个（占 85%），其中互联网上出现“ASUS RT-N12+ B1 权限提升漏洞、SEMCMS SQL 注入漏洞（CNVD-2024-23136）”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 8468 个，与上周（14234 个）环比减少 41%。

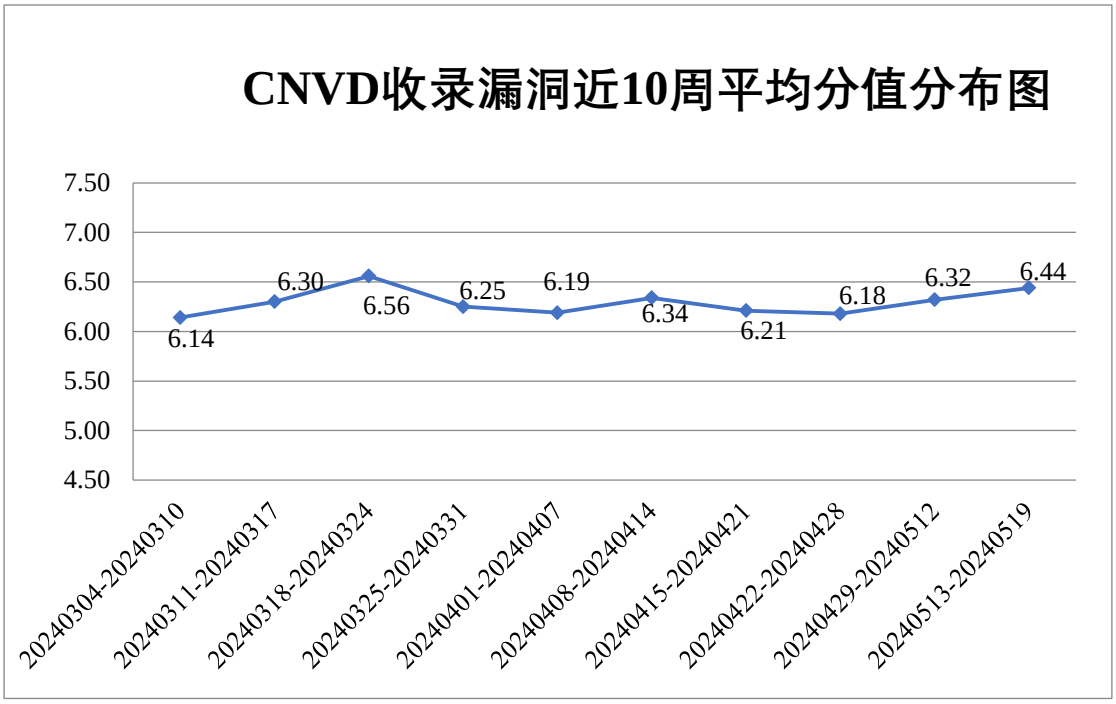

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 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 415 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 60 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 15 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、重庆匠果科技有限公司、中远海运科技股份有限公司、中电鸿信信息科技有限公司、真珍斑马技术贸易（上海）有限公司、浙江和达科技股份有限公司、长沙千视电子科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、银雁科技服务集团股份有限公司、雅马哈乐器音响（中国）投资有限公司、星云海数字科技股份有限公司、信呼、新天科技股份有限公司、夏普商贸（中国）有限公司、西门子（中国）有限公司、西安瑞友信息技术资讯有限公司、武汉秒开网络科技有限公司、温州市易天信息科技有限公司、万洲电气股份有限公司、同望科技股份有限公司、索尼（中国）有限公司、松下电器（中国）有限公司、深圳坐标软件集团有限公司、深圳拓安信物联股份有限公司、深圳市优特普技术有限公司、深圳市同为数码科技股份有限公司、深圳市腾狐物联科技有限公司、深圳市联软科技股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市东宝信息技术有限公司、深圳市必联电子有限公司、深圳警翼智能科技股份有限公司、深圳邦健生物医疗设备股份有限公司 、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海桑锐电子科技股份有限公司、上海华测导航技术股份有限公司、上海费浦安防技术有限公司、上海斐讯数据通信技术有限公司、商派软件有限公司、山脉科技股份有限公司、山东云时空信息科技有限公司、山东潍微科技股份有限公司、山东泰港数字科技集团有限公司、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、融智通科技（北京）股份有限公司、青岛三利集团有限公司、青岛恒泽水利科技有限公司、麒麟软件有限公司、南昌航天广信科技有限责任公司、龙芯开源社区、龙采科技集团有限责任公司、联想集团、柯尼卡美能达办公系统（中国）有限公司、江苏金智教育信息股份有限公司、江苏汇文软件有限公司、嘉和美康（北京）科技股份有限公司、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、湖南建研信息技术股份有限公司、河北先河环保科技股份有限公司、合肥旭冉信息科技有限公司、杭州雄伟科技开发股份有限公司、杭州海康威视数字技术股份有限公司、海通安恒科技股份有限公司、国子软件股份有限公司、广州市和丰自动化科技有限公司、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、烽火通信科技股份有限公司、鼎捷软件股份有限公司、顶点软件股份有限公司、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、北京中成科信科技发展有限公司、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、北京颖杰联创科技有限公司、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、北京五指互联科技有限公司、北京沃丰时代数据科技有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京天融信网络安全技术有限公司、北京神州数码云计算有限公司、北京神州视翰科技有限公司、北京美特软件技术有限公司、北京久其云福科技有限公司、北京久其软件股份有限公司、北京金和网络股份有限公司、北京杰控科技有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、奥琦玮信息科技（北京）有限公司、安元科技股份有限公司、安翼物联网（南京）有限公司、安阳市军博软件有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安徽阳光心健科技发展有限公司、爱普生（中国）有限公司、Semcms 和《中国学术期刊（光盘版）》电子杂志社有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、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、北京数字观星科技有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。西门子（中国）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、北京中睿天下信息技术有限公司、联想集团、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、中资网络信息安全科技有限公司、成都久信信息技术股份有限公司、内蒙古中叶信息技术有限责任公司、重庆都会信息科技有限公司、成都思维世纪科技有限责任公司、北京天防安全科技有限公司、海南神州希望网络有限公司、江苏晟晖信息科技有限公司、河南天祺信息安全技术有限公司、杭州海康威视数字技术股份有限公司、江苏极元信息技术有限公司、湖南泛联新安信息科技有限公司、润成安全技术有限公司、联通数字科技有限公司、成都安美勤信息技术股份有限公司、西藏熙安信息技术有限责任公司、辽宁海事局、北京栖安科技有限责任公司、北京航空航天大学、江苏百达智慧网络科技有限公司、国家能源集团、江西中和证信息安全技术有限公司、上海亿保健康科技集团有限公司、快页信息技术有限公司及其他个人白帽子向 CNVD 提交了 8468 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 7286 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）	4950	4950
奇安信网神（补天平台）	1601	1601
北京天融信网络安全	932	21

技术有限公司		
北京启明星辰信息安全技术有限公司	692	2
三六零数字安全科技集团有限公司	531	531
新华三技术有限公司	258	0
北京数字观星科技有限公司	227	0
上海交大	204	204
阿里云计算有限公司	164	0
华为技术有限公司	102	1
恒安嘉新（北京）科技股份公司	81	0
北京知道创宇信息技术有限公司	64	1
中国电信集团系统集成有限责任公司	14	0
北京安信天行科技有限公司	14	14
杭州迪普科技股份有限公司	10	0
西安四叶草信息技术有限公司	4	4
杭州安恒信息技术股份有限公司	3	3
北京智游网安科技有限公司	2	2
远江盛邦（北京）网络安全科技股份有限公司	1	1
北京长亭科技有限公司	1	1
西门子（中国）有限公司	55	0
河南东方云盾信息技	36	36

术有限公司		
江苏金盾检测技术股份有限公司	29	29
北京中睿天下信息技术有限公司	14	14
联想集团	9	9
安徽天行网安信息安全技术有限公司	8	8
中国电信股份有限公司上海研究院	7	7
中资网络信息安全科技有限公司	7	7
成都久信信息技术股份有限公司	6	6
内蒙古中叶信息技术有限责任公司	6	6
重庆都会信息科技有限公司	6	6
成都思维世纪科技有限责任公司	4	4
北京天防安全科技有限公司	3	3
海南神州希望网络有限公司	3	3
江苏晟晖信息科技有限公司	3	3
河南天祺信息安全技术有限公司	2	2
杭州海康威视数字技术股份有限公司	2	2
江苏极元信息技术有限公司	2	2
湖南泛联新安信息科技有限公司	2	2
润成安全技术有限公	2	2

司		
联通数字科技有限公司	2	2
成都安美勤信息技术股份有限公司	2	2
西藏熙安信息技术有限责任公司	2	2
辽宁海事局	2	2
北京栖安科技有限责任公司	1	1
北京航空航天大学	1	1
江苏百达智慧网络科技有限公司	1	1
国家能源集团	1	1
江西中和证信息安全技术有限公司	1	1
上海亿保健康科技集团有限公司	1	1
快页信息技术有限公司	1	1
CNCERT 河北分中心	2	2
CNCERT 贵州分中心	2	2
个人	962	962
报送总计	11042	8468

本周漏洞按类型和厂商统计

本周，CNVD 收录了 696 个漏洞。WEB 应用 359 个，网络设备（交换机、路由器等网络端设备）136 个，应用程序 123 个，智能设备（物联网终端设备）50 个，操作系统 17 个，安全产品 8 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	359
网络设备（交换机、路由器等网络端设备）	136
应用程序	123

智能设备（物联网终端设备）	50
操作系统	17
安全产品	8
数据库	3

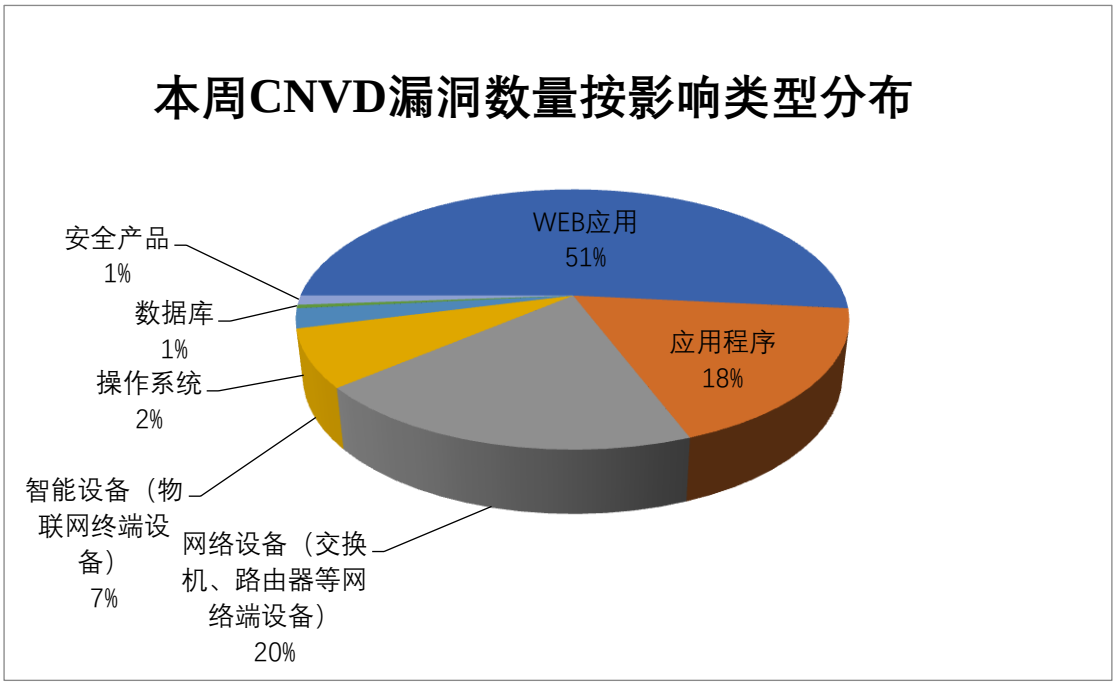

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用友网络科技股份有限公司、北京星网锐捷网络技术有限公司、北京金和网络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	用友网络科技股份有限公司	24	4%
2	北京星网锐捷网络技术有限公司	23	3%
3	北京金和网络股份有限公司	18	3%
4	北京百卓网络技术有限公司	16	2%
5	Apache	16	2%
6	Tenda	15	2%
7	北京亿赛通科技发展有限责任公司	15	2%
8	IBM	14	2%

9	爱普生（中国）有限公司	13	2%
10	其他	542	78%

本周行业漏洞收录情况

本周，CNVD 收录了 60 个电信行业漏洞，32 个移动互联网行业漏洞，16 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-845L 命令执行漏洞、Siemens Parasolid X_T 文件越界读取漏洞”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/

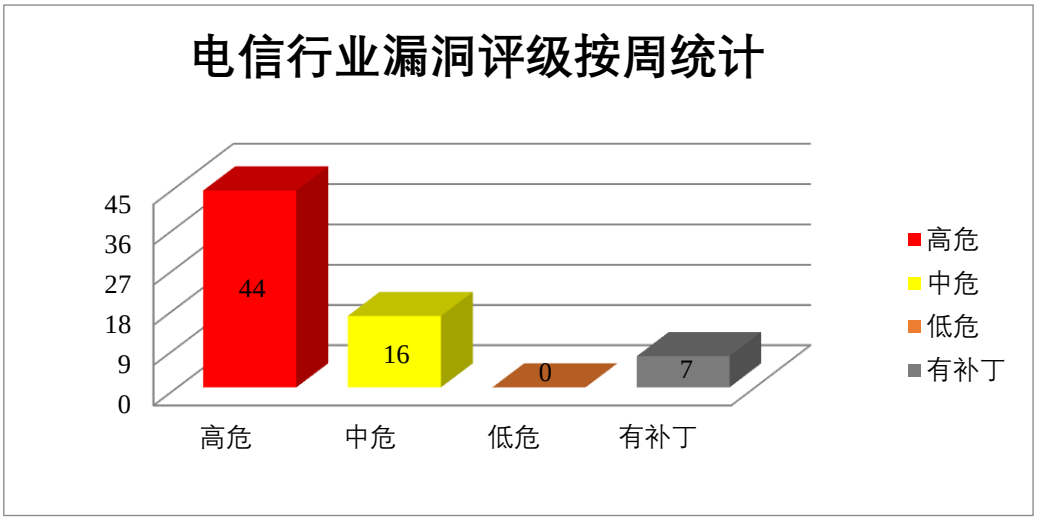

图 3 电信行业漏洞统计

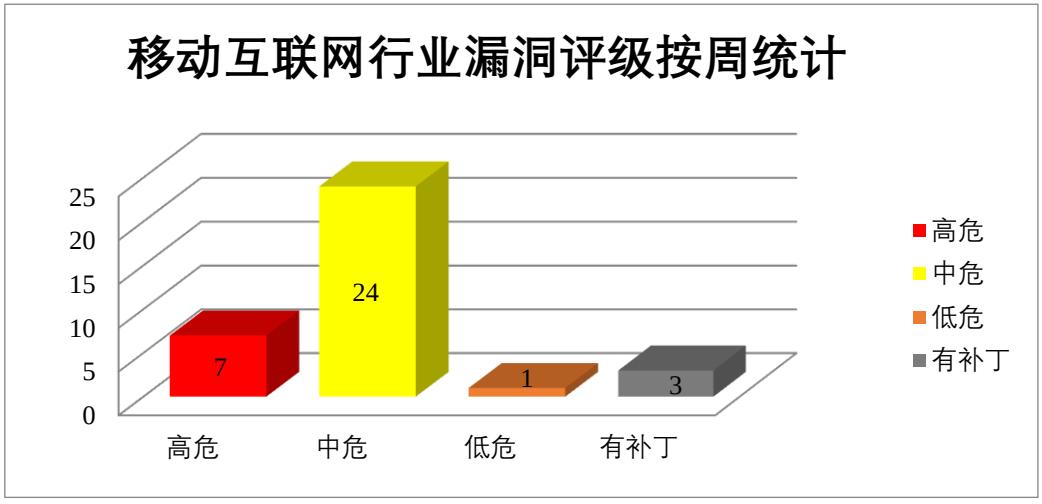

图 4 移动互联网行业漏洞统计

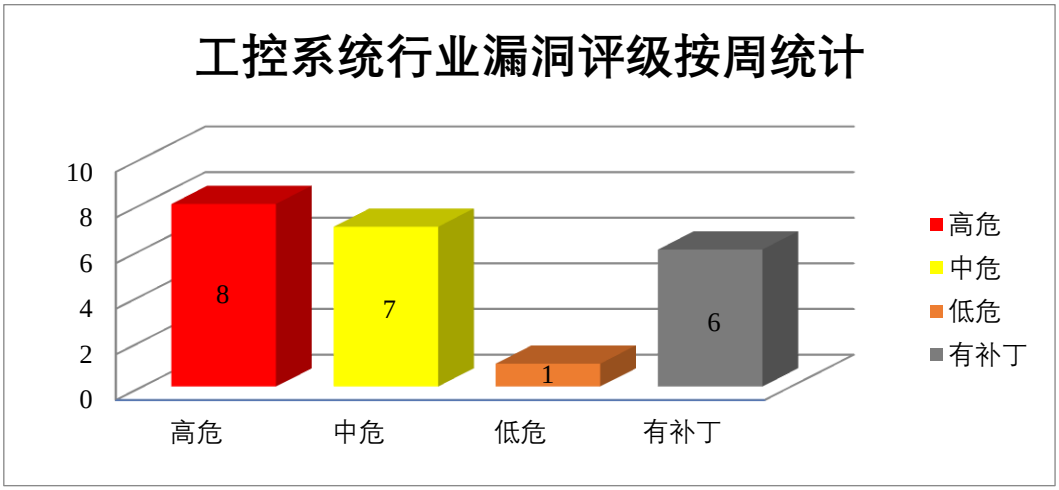

图 5 工控系统行业漏洞统计

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、Apache 产品安全漏洞

Apache InLong 是美国阿帕奇（Apache）基金会的一站式的海量数据集成框架。提供自动化、安全、可靠的数据传输能力。Apache Zookeeper 是一个软件项目，它能够为大型分布式计算提供开源的分布式配置服务、同步服务和命名注册等功能。Apache CXF 是一个开源的 Web 服务框架。该框架支持多种 Web 服务标准、多种前端编程 API 等。Apache NimBLE 是一个开源蓝牙 5.4 堆栈（主机和控制器），完全取代 Nordic 芯片组上的专有 SoftDevice。它是 Apache Mynewt 项目的一部分。Apache Ambari 是一个应用软件。提供开发用于配置，管理和监视 Apache Hadoop 集群的软件来简化 Hadoop 管理。Apache Airflow 是一套用于创建、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 Kylin 是一款开源的分布式分析型数据仓库。该产品主要提供 Hadoop/Spark 之上的 SQL 查询接口及多维分析（OLAP）等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取 znodes 的完整路径信息，通过发送特制请求，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Apache InLong 代码执行漏洞（CNVD-2024-22229）、Apache ZooKeeper 信息泄露漏洞（CNVD-2024-22232）、Apache CXF 服务器端请求伪造漏洞、Apache NimBLE 拒绝服务漏洞、Apache Ambari 跨站脚本漏洞（CNVD-2024-22235）、Apache Airflow 信息泄露漏洞（CNVD-2024-22234）、Apache Kylin 信息泄露漏洞（CNVD-2024-22238）、Apache Ambari 代码注入漏洞。其中，“Apache InLong 代码执行漏洞（CNVD-2024-22229）、Apache NimBLE 拒绝服务漏洞、Apache Kylin 信息泄露漏洞（CNVD-2024-22238）、Apache Ambari 代码注入漏洞”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-2024-22229

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22232

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22231

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22230

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22235

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22234

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22238

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22237

2、IBM 产品安全漏洞

IBM Cognos Controller 是美国国际商业机器（IBM）公司的一套商业智能与计划解决方案。该产品具有流程自动化、财务审计控制、创建和管理财务报告等功能。IBM Aspera 是一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。IBM MQ Appliance 是一款用于快速部署企业级消息中间件的一体机设备。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，导致拒绝服务，提升权限，通过发送特制请求在系统上执行任意命令等。

CNVD 收录的相关漏洞包括：IBM Cognos Controller 访问控制错误漏洞、IBM Cognos Controller 代码执行漏洞、IBM Aspera 操作系统命令注入漏洞、IBM Aspera Faspex 拒绝服务漏洞、IBM Aspera Faspex 权限提升漏洞、IBM MQ Appliance 缓冲区溢出漏洞（CNVD-2024-22243）、IBM Aspera Faspex 日志信息泄露漏洞、IBM Aspera Faspex 加密问题漏洞。其中，“IBM Aspera 操作系统命令注入漏洞、IBM MQ Appliance 缓冲区溢出漏洞（CNVD-2024-22243）”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-2024-22241

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22240

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22239

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22246

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22245

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22243

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22249

https://www.cnvd.org.cn/flaw/show/CNVD-2024-22247

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。Adobe Lightroom Desktop 是一款专业的照片管理和编辑软件，旨在为摄影师和图像编辑人员提供强大的工作流程和编辑工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞将恶意脚本注入易受攻击的网页中，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-22221、CNVD-2024-22220、CNVD-2024-22219、CNVD-2024-22225、CNVD-2024-22224、CNVD-2024-22223、CNVD-2024-22226）、Adobe Lightroom Desktop 代码问题漏洞。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-2024-22221
https://www.cnvd.org.cn/flaw/show/CNVD-2024-22220
https://www.cnvd.org.cn/flaw/show/CNVD-2024-22219
https://www.cnvd.org.cn/flaw/show/CNVD-2024-22225
https://www.cnvd.org.cn/flaw/show/CNVD-2024-22224
https://www.cnvd.org.cn/flaw/show/CNVD-2024-22223
https://www.cnvd.org.cn/flaw/show/CNVD-2024-22227
https://www.cnvd.org.cn/flaw/show/CNVD-2024-22226

4、 Siemens 产品安全漏洞

Siemens Parasolid 是一种三维几何建模工具，支持各种技术，包括实体建模、直接编辑和自由曲面/图纸建模。Siemens Tecnomatix Plant Simulation 是一个工控设备。利用离散事件仿真的功能进行生产量分析和优化，进而改善制造系统性能。Siemens Solid Edge 是一款三维 CAD 软件。该软件可用于零件设计、装配设计、钣金设计、焊接设计等行业。SIMATIC RTLS Locating Manager 用于配置、操作和维护 SIMATIC RTLS 装置，该装置是一个实时无线定位系统，可提供定位解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞窃听和修改传输中的资源，在当前进程的上下文中执行代码等。

CNVD 收录的相关漏洞包括：Siemens Parasolid X_T 文件越界读取漏洞（CNVD-2024-23105、CNVD-2024-23106）、Siemens Parasolid X_T 文件越界写入漏洞、Siemens Tecnomatix Plant Simulation MODEL 文件越界写入漏洞、Siemens Solid Edge 堆缓冲区溢出漏洞（CNVD-2024-23110）、Siemens Solid Edge 越界读取漏洞（CNVD-2024-23111、CNVD-2024-23112）、Siemens SIMATIC RTLS Locating Manager 敏感信息明文传输漏洞。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-2024-23105
https://www.cnvd.org.cn/flaw/show/CNVD-2024-23106

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23108

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23109

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23110

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23111

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23112

https://www.cnvd.org.cn/flaw/show/CNVD-2024-23116

5、NETGEAR DG834G 信息泄露漏洞

NETGEAR DG834G 是美国网件（NETGEAR）公司的一款无线 ADSL 防火墙调制解调器。本周，NETGEAR DG834G 被披露存在信息泄露漏洞。攻击者可利用该漏洞可以获取设备的管理访问权限。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-2024-22869

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-2024-22229	Apache InLong 代码执行漏洞（CNVD-2024-22229）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://inlong.apache.org/
CNVD-2024-22230	Apache NimBLE 拒绝服务漏洞	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/bptkzc0o2ymjk8qqzqdmy39kcmh27078
CNVD-2024-22237	Apache Ambari 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://cwiki.apache.org/confluence/display/AMBARI/Installation+Guide+for+Ambari+2.7.8
CNVD-2024-22239	IBM Aspera 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7150117
CNVD-2024-22243	IBM MQ Appliance 缓冲区溢出漏洞（CNVD-2024-22243）	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/7149481
CNVD-2024-23105	Siemens Parasolid X_T 文件越界读取漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/produ

			ctcert/html/ssa-046364.html
CNVD-2024-23108	Siemens Parasolid X_T 文件越界写入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-489698.html
CNVD-2024-23110	Siemens Solid Edge 堆缓冲区溢出漏洞（CNVD-2024-23110）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-589937.html
CNVD-2024-23112	Siemens Solid Edge 越界读取漏洞（CNVD-2024-23112）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-589937.html
CNVD-2024-23132	D-Link DIR-845L 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.dlink.com/uk/en/products/dir-845l-cloud-gigabit-router-n600-with-smartbeam-technology

小结：本周，Apache 产品被披露存在多个漏洞，攻击者可利用漏洞获取 znodes 的完整路径信息，通过发送特制请求，在系统上执行任意代码等。此外，IBM、Adobe、Siemens 等多款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，导致拒绝服务，在当前进程的上下文中执行代码等。另外，NETGEAR DG834G 被披露存在信息泄露漏洞。攻击者可利用该漏洞可以获取设备的管理访问权限。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、SEMCMS SQL 注入漏洞（CNVD-2024-23136）

验证描述

SEMCMS 是一套支持多种语言的外贸网站内容管理系统（CMS）。

SEMCMS 4.8 及之前版本存在 SQL 注入漏洞，该漏洞源于应用缺少对外部输入 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/gatsby2003/Semcms/blob/main/semcms0-sqlinjection.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-23136

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. 新的 Wi-Fi 漏洞通过降级攻击启用网络窃听

研究人员发现了一个新的安全漏洞，该漏洞源于 IEEE 802.11 Wi-Fi 标准中的设计缺陷，该缺陷诱骗受害者连接到安全性较低的无线网络并窃听他们的网络流量。SSID 混淆攻击被跟踪为 CVE-2023-52424，影响所有操作系统和 Wi-Fi 客户端，包括基于 WEP、WPA3、802.11X/EAP 和 AMPE 协议的家庭和网状网络。

参考链接：https://thehackernews.com/2024/05/new-wi-fi-vulnerability-enabling.html

2. 研究人员发现 GE 医疗超声机的 11 个安全漏洞

安全研究人员已经披露了近十几个影响 GE HealthCare Vivid Ultrasound 产品系列的安全漏洞，恶意行为者可能会利用这些漏洞篡改患者数据，甚至在某些情况下安装勒索软件。

参考链接：https://thehackernews.com/2024/05/researchers-uncover-11-security-flaws.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