国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 04 月 01 日-2024 年 04 月 07 日 **2024 年第 14 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 480 个，其中高危漏洞 185 个、中危漏洞 281 个、低危漏洞 14 个。漏洞平均分值为 6.19。本周收录的漏洞中，涉及 0day 漏洞 434 个（占 90%），其中互联网上出现“Library Management System Student 参数 SQL 注入漏洞、JFinalCMS SQL 注入漏洞（CNVD-2024-15735）”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 6454 个，与上周（11801 个）环比减少 45%。

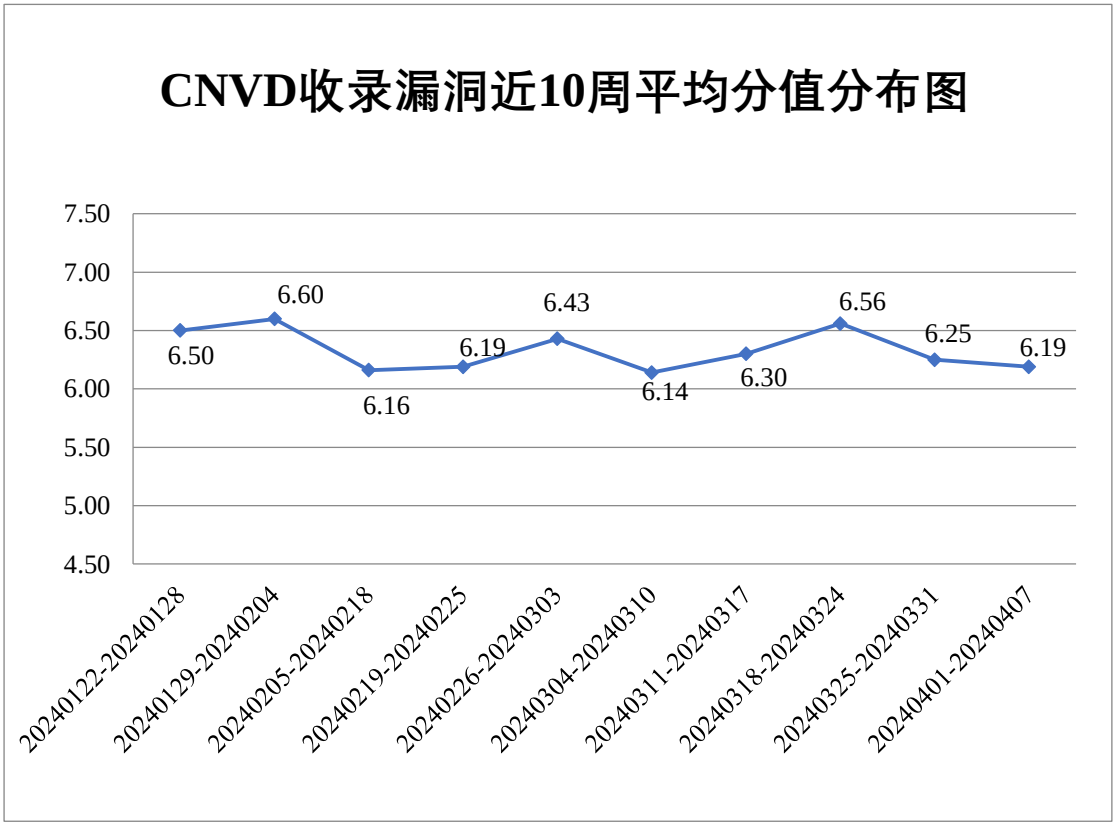

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 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 295 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 35 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 31 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：

紫兴科技集团有限公司、紫光软件系统有限公司、珠海金山办公软件有限公司、智恒科技股份有限公司、正元智慧集团股份有限公司、浙江律联信息科技有限公司、浙江和达科技股份有限公司、浙江电子口岸有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、宜昌云启互联技术中心有限公司、新都（青岛）办公系统有限公司、新东润地产有限公司、西安博达软件股份有限公司、武汉海昌信息技术有限公司、万洲电气股份有限公司、统信软件技术有限公司、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、视联动力信息技术股份有限公司、世邦通信股份有限公司、神州数码控股有限公司、深圳誉龙数字技术有限公司、深圳希施玛数据科技有限公司、深圳维盟网络技术有限公司、深圳市中电数通智慧安全科技股份有限公司、深圳市云之声科技有限公司、深圳市唯德科创信息有限公司、深圳市思迅软件股份有限公司、深圳市锐明技术股份有限公司、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、深圳市汇川技术股份有限公司、深圳市道尔智控科技股份有限公司、深圳齐心好视通云计算有限公司、深圳力维智联技术有限公司、申瓯通信设备有限公司、上海纵之格科技有限公司、上海易正信息技术有限公司、上海迅饶自动化科技有限公司、上海玄科计算机技术有限公司、上海尚强信息科技有限公司、上海商派网络科技有限公司、上海灵当信息科技有限公司、上海肯特仪表股份有限公司、上海金电网安科技有限公司、上海寰创通信科技股份有限公司、上海泛微网络科技股份有限公司、上海博达数据通信有限公司、山西牛之云网络科技有限公司、山西牛酷信息科技有限公司、山脉科技股份有限公司、山东国子软件股份有限公司、山东比特智能科技股份有限公司、厦门泰博科技有限公司、厦门四联信息技术有限公司、确信信息股份有限公司、青岛紫霄网络科技有限公司、青岛和正信息技术有限公司、青岛海威茨仪表有限公司、麒麟软件有限公司、南京云网汇联软件技术有限公司、南京易联阳光信息技术股份有限公司、南京先维信息技术有限公司、南昌航天广信科技有限责任公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、力新国际科技股份有限公司、蓝网科技股份有限公司、开放原子开源基金会、江苏群杰物联科技有限公司、江苏金智教育信息股份有限公司、吉翁电子（深圳）有限公司、华新智科技产业发展股份有限公司、湖南强智科技发展有限公司、河北先河环保科技股份有限公司、杭州易软共创网络科技有限公司、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、杭州睿贝科技有限公司、杭州翰阳科技有限公司、杭州恩软信息技术有限公司、广州志华软件科技有限公司、广州小橘灯信息科技有限公司、广州图创计算机软件开发有限公司、广联达科技股份有限公司、高新兴科技集团股份有限公司、福建科立讯通信有限公司、东莞市东城飞飞网络科技经营部、大连金马衡器有限公司、成都飞鱼星科技股份有限公司、郴州帝云网络科技有限公司、畅捷通信息技术股份有限公司、禅道软件（青岛）有限公司、北京中科聚网信息技术有限公司、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、北京雪迪龙科技股份有限公司、北京熊宝贝科技发展有限公司、北京星网锐捷网络技术有限公司、北京万维盈创科技发展有限公司、北京通达信科科技有限公司、北京霆智科技有限公司、北京派网软件有限公司、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、北京火绒网络科技有限公司、北京超粮科技有限责任公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、安元科技股份有限公司、安翼物联网（南京）有限公司、安美世纪（北京）科技有限公司、爱德克电气贸易（上海）有限公司和艾波蘿網站設計有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、天津市国瑞数码安全系统股份有限公司、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、安徽天行网安信息安全技术有限公司、内蒙古中叶信息技术有限责任公司、河南东方云盾信息技术有限公司、快页信息技术有限公司、西藏熙安信息技术有限责任公司、河南灵创电子科技有限公司、贵州多彩网安科技有限公司、联想集团、甘肃赛飞安全科技有限公司、浙江谦卦信息科技有限公司、中孚安全技术有限公司、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、北京微步在线科技有限公司、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、杭州海康威视数字技术股份有限公司、北京时代新威信息技术有限公司、江苏晟晖信息科技有限公司、上海观安信息技术股份有限公司、北京卓识网安技术股份有限公司、中华人民共和国上海海事局、信联科技（南京）有限公司、联通数字科技有限公司、山石网科通信技术股份有限公司、北京星网锐捷网络技术有限公司、北京六方云信息技术有限公司、北京山石网科信息技术有限公司及其他个人白帽子向 CNVD 提交了 6454 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 5583 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）	3623	3623
奇安信网神（补天平台）	1045	1045
上海交大	915	915
北京启明星辰信息安全技术有限公司	554	3
北京天融信网络安全技术有限公司	529	0
新华三技术有限公司	426	0
天津市国瑞数码安全系统股份有限公司	381	0
安天科技集团股份有限公司	237	0
深信服科技股份有限公司	87	0
华为技术有限公司	78	0
恒安嘉新（北京）科技股份公司	31	0
中国电信集团系统集成有限责任公司	30	0
杭州安恒信息技术股份有限公司	17	17
北京安信天行科技有限公司	10	10
杭州迪普科技股份有限公司	6	0
阿里云计算有限公司	5	5
北京知道创宇信息技术有限公司	5	5
北京长亭科技有限公司	2	1
北京智游网安科技有限公司	1	1
江苏金盾检测技术股份有限公司	67	67

安徽天行网安信息安全技术有限公司	21	21
内蒙古中叶信息技术有限责任公司	9	9
河南东方云盾信息技术有限公司	8	8
快页信息技术有限公司	8	8
西藏熙安信息技术有限责任公司	7	7
河南灵创电子科技有限公司	7	7
贵州多彩网安科技有限公司	6	6
联想集团	6	6
甘肃赛飞安全科技有限公司	5	5
浙江谦卦信息科技有限公司	3	3
中孚安全技术有限公司	3	3
中国电信股份有限公司上海研究院	3	3
中资网络信息安全科技有限公司	2	2
北京微步在线科技有限公司	2	2
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
杭州海康威视数字技术股份有限公司	1	1
北京时代新威信息技术有限公司	1	1

江苏晟晖信息科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
北京卓识网安技术股份有限公司	1	1
中华人民共和国上海海事局	1	1
信联科技（南京）有限公司	1	1
联通数字科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京星网锐捷网络技术有限公司	1	1
北京六方云信息技术有限公司	1	1
北京山石网科信息技术有限公司	1	1
个人	658	658
报送总计	8811	6454

本周漏洞按类型和厂商统计

本周，CNVD 收录了 480 个漏洞。WEB 应用 244 个，应用程序 119 个，网络设备（交换机、路由器等网络端设备）81 个，操作系统 13 个，数据库 10 个，智能设备（物联网终端设备）7 个，安全产品 6 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	244
应用程序	119
网络设备（交换机、路由器等网络端设备）	81
操作系统	13
数据库	10
智能设备（物联网终端设备）	7

安全产品	6

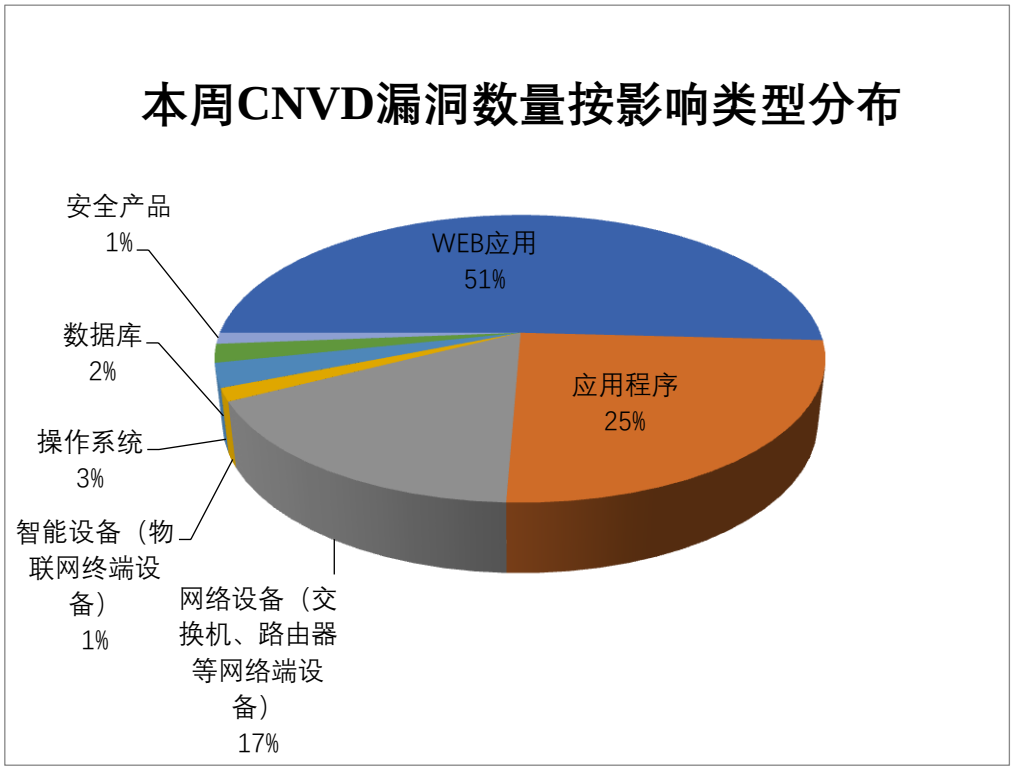

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及杭州恩软信息技术有限公司、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	杭州恩软信息技术有限公司	22	5%
2	用友网络科技股份有限公司	17	4%
3	北京星网锐捷网络技术有限公司	14	3%
4	新华三技术有限公司	12	2%
5	Apache	11	2%
6	DELL	11	2%
7	雅马哈乐器音响（中国）投资有限公司	10	2%
8	广州图创计算机软件开发有限公司	10	2%
9	IBM	9	2%

10	其他	364	76%

本周行业漏洞收录情况

本周，CNVD 收录了 39 个电信行业漏洞，49 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Rockwell Automation 1756 EN2 and 1756 EN3 拒绝服务漏洞”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/

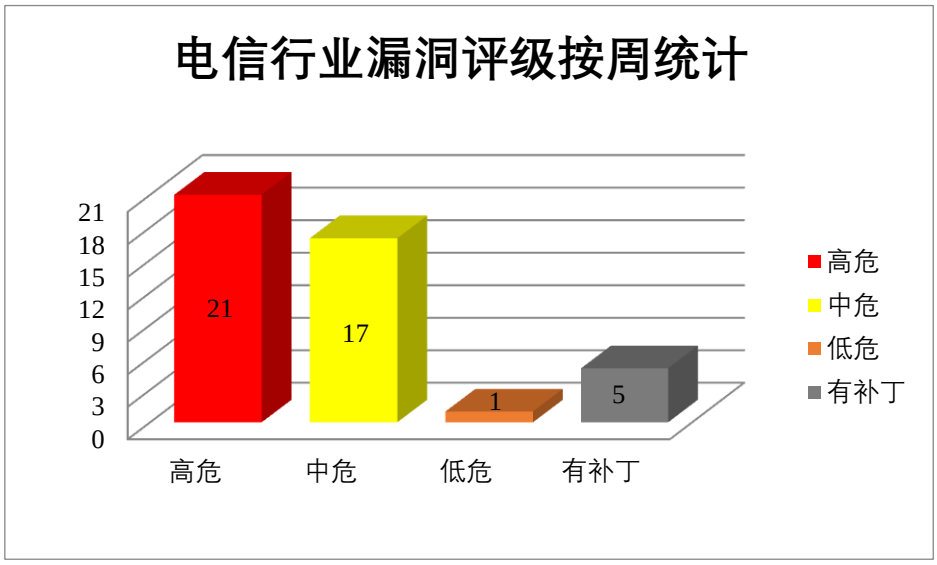

图 3 电信行业漏洞统计

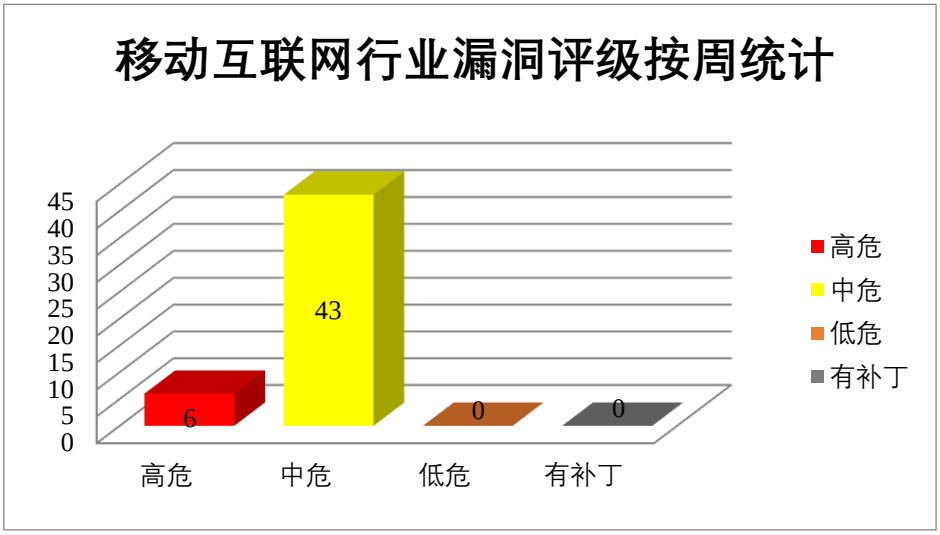

图 4 移动互联网行业漏洞统计

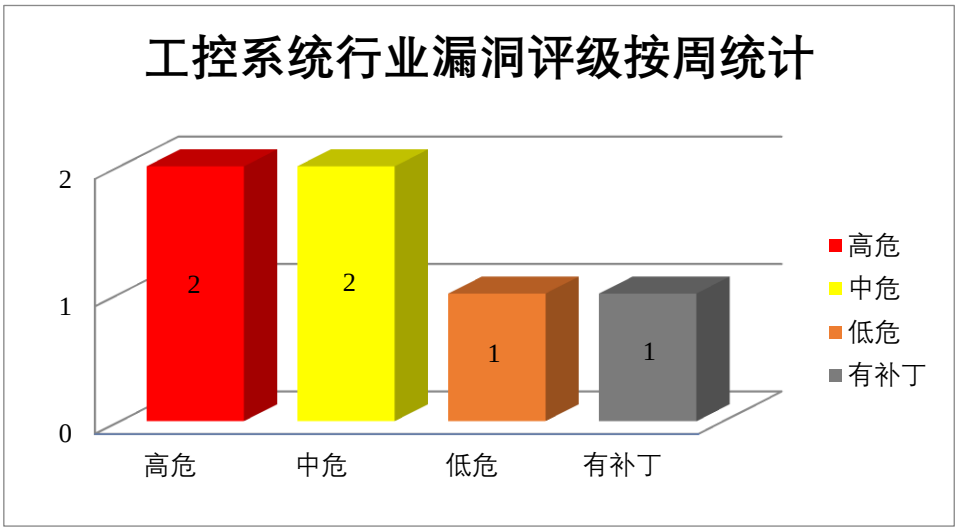

图 5 工控系统行业漏洞统计

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 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 Directory 是美国国际商业机器（IBM）公司的一款身份验证和访问管理解决方案的一部分。IBM Common Cryptographic Architecture 是美国国际商业机器（IBM）公司的一个密码平台。提供一些功能来保护金融交易。IBM WebSphere Application Server Liberty 是美国国际商业机器（IBM）公司的一款构建于 Open Liberty 项目之上的 Java 应用程序服务器。IBM Cognos Analytics 是美国国际商业机器（IBM）公司的一套商业智能软件。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。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，导致拒绝服务，构建恶意 URI，诱使请求，可以目标用户上下文执行恶意操作等。

CNVD 收录的相关漏洞包括：IBM QRadar SIEM 跨站脚本漏洞（CNVD-2024-15726、CNVD-2024-15725）、IBM Security Verify Directory 加密问题漏洞、IBM Security Verify Directory 跨站脚本漏洞、IBM Common Cryptographic Architecture 资源管理错误漏洞、IBM WebSphere Application Server Liberty 跨站脚本漏洞（CNVD-2024-15727）、IBM Cognos Analytics 表单跨站请求伪造漏洞、IBM Aspera SQL 注入漏洞。其中，“IBM Common Cryptographic Architecture 资源管理错误漏洞、IBM Aspera SQL 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-2024-15726

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15725

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15730

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15729

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15728

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15727

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15733

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15731

2、 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 Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。Adobe Substance 3D Painter 是美国奥多比（Adobe）公司的一个 3D 纹理处理应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞将恶意脚本注入易受攻击的网页中，导致敏感内存泄露，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-2024-15718、CNVD-2024-15717、CNVD-2024-15719、CNVD-2024-15723）、Adobe Animate 缓冲区溢出漏洞（CNVD-2024-15721、CNVD-2024-15720、CNVD-2024-15722）、Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-15724）。其中，“Adobe Animate 缓冲区溢出漏洞（CNVD-2024-15720）”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-2024-15718

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15717

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15721

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15720

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15719

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15723

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15722

https://www.cnvd.org.cn/flaw/show/CNVD-2024-15724

3、 Apache 产品安全漏洞

Apache Fineract 是美国阿帕奇（Apache）基金会的一套开源数字金融服务平台。该平台能够为用户提供数据管理、贷款和储蓄投资组合管理以及实时财务数据等功能。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。Apache Commons Configuration 是美国阿帕奇（Apache）基金会的一款通用的配置接口，它主要用于使 Java 应用程序从多种来源读取配置数据。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。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请求，在系统上执行任意代码，发送特制的有效负载，读取系统上的任意文件等。

CNVD 收录的相关漏洞包括：Apache Fineract 权限提升漏洞、Apache Fineract SQL 注入漏洞（CNVD-2024-16107、CNVD-2024-16106）、Apache Doris 命令执行漏洞、Apache Doris 安全绕过漏洞、Apache Commons Configuration 越界写入漏洞（CNVD-2024-16110、CNVD-2024-16109）、Apache InLong 代码问题漏洞（CNVD-2024-16113）。其中，“Apache Fineract SQL 注入漏洞（CNVD-2024-16107、CNVD-2024-16106）、Apache Commons Configuration 越界写入漏洞（CNVD-2024-16109、CNVD-2024-16110）”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-2024-16108

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16107

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16106

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16112

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16111

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16110

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16109

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16113

4、DELL 产品安全漏洞

Dell InsightIQ 是美国戴尔（Dell）公司的一个性能监控和报告工具。Dell PowerScale OneFS 是美国戴尔（Dell）公司的一个操作系统。提供横向扩展 NAS 的 PowerScale OneFS 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未经授权的访问监控数据，导致拒绝服务，导致权限升级等。

CNVD 收录的相关漏洞包括：Dell InsightIQ 访问控制错误漏洞、Dell PowerScale OneFS 明文传输敏感信息漏洞、Dell PowerScale OneFS 加密问题漏洞（CNVD-2024-16188）、Dell PowerScale OneFS 代码问题漏洞、Dell PowerScale OneFS 日志信息泄露漏洞（CNVD-2024-16190）、Dell PowerScale OneFS 不正确权限管理漏洞、Dell PowerScale OneFS 拒绝服务漏洞（CNVD-2024-16219）、Dell PowerScale OneFS 信息泄露漏洞（CNVD-2024-16220）。其中，“Dell InsightIQ 访问控制错误漏洞、Dell PowerScale OneFS 明文传输敏感信息漏洞、Dell PowerScale OneFS 信息泄露漏洞（CNVD-2024-16220）”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-2024-15739

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16187

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16188

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16189

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16190

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16192

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16219

https://www.cnvd.org.cn/flaw/show/CNVD-2024-16220

5、Online Book System cart.php 文件 SQL 注入漏洞

Online Book System 是一个在线预定系统。本周，Online Book System 被披露存在 SQL 注入漏洞。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。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-2024-15741

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-2024-16106	Apache Fineract SQL 注入漏洞（CNVD-2024-16106）	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/g8sv1gnjv716lx2h89jbvjdgtrrjmy7h
CNVD-2024-16107	Apache Fineract SQL 注入漏洞（CNVD-2024-16107）	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/by32w2dylzgbqm5940x3wj7519wolqxs
CNVD-2024-16187	Dell PowerScale OneFS 明文传输敏感信息漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000223366/dsa-2024-115-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities
CNVD-2024-15739	Dell InsightIQ 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000223551/dsa-2024-134-security-update-for-dell-insightiq-for-proprietary-code-vulnerability
CNVD-2024	IBM Common Cryptographic	高	厂商已发布了漏洞修复程序，请及

-15728	Architecture 资源管理错误漏洞		时关注更新：https://www.ibm.com/support/pages/node/7145168
CNVD-2024-16109	Apache Commons Configuration 越界写入漏洞（CNVD-2024-16109）	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/ccb9w15bscznh6tnp3wsvrrj9crbszh2
CNVD-2024-16110	Apache Commons Configuration 越界写入漏洞	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/03nzzzjn4oknyw5y0871tw7ltj0t3r37
CNVD-2024-15720	Adobe Animate 缓冲区溢出漏洞（CNVD-2024-15720）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/animate/apsb24-19.html
CNVD-2024-15731	IBM Aspera SQL 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/7122632
CNVD-2024-16220	Dell PowerScale OneFS 信息泄露漏洞（CNVD-2024-16220）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000222691/dsa-2024-062-security-update-for-dell-powerscale-onefs-for-proprietary-code-vulnerabilities

小结：本周，IBM 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，导致拒绝服务，构建恶意 URI，诱使请求，可以目标用户上下文执行恶意操作等。此外，Adobe、Apache、DELL 等多款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，导致敏感内存泄露，在当前用户的上下文中执行任意代码等。另外，Online Book System 被披露存在 SQL 注入漏洞。攻击者可利用漏洞执行非法 SQL 命令窃取数据库敏感数据。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 Student 参数 SQL 注入漏洞

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 2.0 版本存在 SQL 注入漏洞，该漏洞源于 login.php 文件 Student 参数缺少对外部输入 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-2.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-16840

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. YouTube 被用于传播恶意软件

网络安全公司 Proofpoint 警告称，信息窃取恶意软件正在以盗版软件和视频游戏破解的“幌子”通过 YouTube 传播。该公司在调查后透露，包括 Vidar、StealC 和 Lumma Stealer 在内的恶意软件已以视频游戏破解的形式在 YouTube 上传播。

参考链接：https://cybernews.com/security/youtube-used-to-distribute-malware/

2. 癌症治疗中心 City of Hope 被黑客攻破，82,7 万人隐私信息暴露

虽然调查仍在进行中，但迄今为止确定的受影响个人信息因人而异，但可能包括姓名、联系信息（例如，电子邮件地址、电话号码）、出生日期、社会安全号码、驾驶执照或其他政府身份证明、财务详细信息（例如，银行帐号和/或信用卡详细信息）等。

参考链接：https://cybernews.com/security/cancer-treatment-center-city-of-hope-breach/

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