国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 10 月 21 日-2021 年 10 月 27 日 **2024 年第 43 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 312 个，其中高危漏洞 147 个、中危漏洞 145 个、低危漏洞 20 个。漏洞平均分值为 6.47。本周收录的漏洞中，涉及 0day 漏洞 187 个（占 60%），其中互联网上出现“JEPaaS SQL 注入漏洞、TaskMatic SQL 注入漏洞”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 5074 个，与上周（5533 个）环比减少 8%。

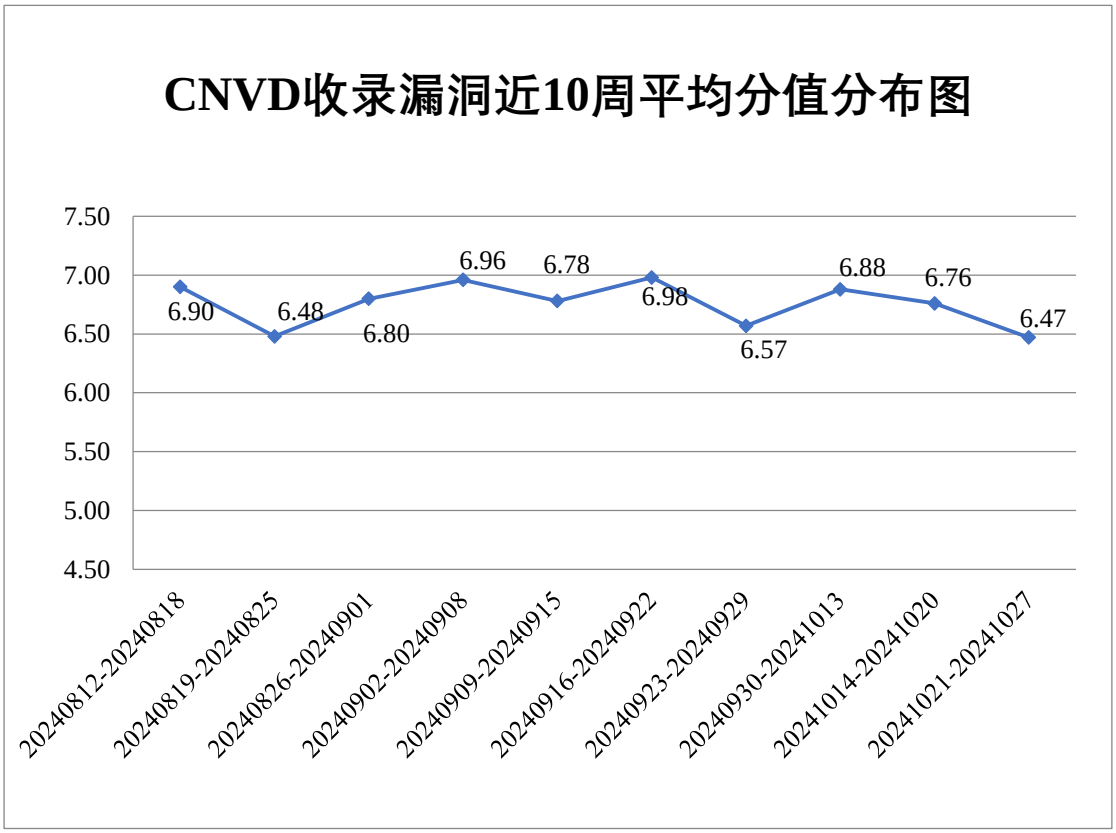

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 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 1154 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 126 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 26 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、浙江大华技术股份有限公司、有智有爱（湖北）医药科技有限公司、用友网络科技股份有限公司、小米科技有限责任公司、武汉良师在线教育科技有限公司、无锡信捷电气股份有限公司、通州区华丽软件工作室、天津蓝点软件开发有限公司、天津环球磁卡集团有限公司、天健软件（常州）有限公司、腾讯安全应急响应中心、深圳市紫光照明技术股份有限公司、深圳勤杰软件有限公司、深圳力维智联技术有限公司、上海穆云智能科技有限公司、上海灵当信息科技有限公司、上海九翊软件科技有限公司、上海华测导航技术股份有限公司、上海布雷德科技有限公司、上海艾泰科技有限公司、山东点狮信息科技有限公司、莆田市飞悦科技有限公司、南京云网汇联软件技术有限公司、迈安德集团有限公司、龙采科技集团有限责任公司、联想安全实验室、科华数据股份有限公司、济南博观智能科技有限公司、河南德尔康药业有限公司、杭州海康威视数字技术股份有限公司、广西天生创想信息技术有限公司、广东保伦电子股份有限公司、懂微信息技术（上海）有限公司、东莞市宇腾信息科技有限公司、畅捷通信息技术股份有限公司、禅道软件（青岛）有限公司、北京中广上洋科技股份有限公司、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、北京网际思安科技有限公司、北京神州视翰科技有限公司、北京南琼电子有限责任公司、北京九思协同软件有限公司、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、百望股份有限公司和安徽银通物联有限公司。

本周，CNVD 发布了《关于 VMware vCenter Server 存在堆溢出漏洞的安全公告》，详情参见 CNVD 网站公告内容（https://www.cnvd.org.cn/webinfo/show/10536）。

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、新华三技术有限公司、安天科技集团股份有限公司、深信服科技股份有限公司、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。中孚安全技术有限公司、河南东方云盾信息技术有限公司、淮安易云科技有限公司、北京山石网科信息技术有限公司、江苏金盾检测技术股份有限公司、江苏云天网络安全技术有限公司、北京珞安科技有限责任

公司及其他个人白帽子向 CNVD 提交了 5074 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）、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 4630 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）	3824	3824
北京启明星辰信息安全技术有限公司	1118	0
新华三技术有限公司	1008	0
安天科技集团股份有限公司	801	0
三六零数字安全科技集团有限公司	495	495
上海交大	311	311
深信服科技股份有限公司	297	0
北京数字观星科技有限公司	252	0
阿里云计算有限公司	165	0
北京神州绿盟科技有限公司	135	135
北京知道创宇信息技术有限公司	129	0
南京众智维信息科技有限公司	103	4
恒安嘉新（北京）科技股份公司	34	0
远江盛邦（北京）网络安全科技股份有限公司	16	16
杭州迪普科技股份有限公司	10	0
北京长亭科技有限公司	5	0
北京升鑫网络科技有	2	2

限公司（青藤云）		
成都卫士通信息安全技术有限公司	39	39
中孚安全技术有限公司	15	15
河南东方云盾信息技术有限公司	14	14
淮安易云科技有限公司	7	7
西门子（中国）有限公司	4	0
北京山石网科信息技术有限公司	3	3
江苏金盾检测技术股份有限公司	3	3
江苏云天网络安全技术有限公司	1	1
北京珞安科技有限责任公司	1	1
个人	204	204
报送总计	8996	5074

本周漏洞按类型和厂商统计

本周，CNVD 收录了 312 个漏洞。WEB 应用 172 个，应用程序 64 个，网络设备（交换机、路由器等网络端设备）34 个，操作系统 16 个，智能设备（物联网终端设备）12 个，安全产品 7 个，数据库 7 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	172
应用程序	64
网络设备（交换机、路由器等网络端设备）	34
操作系统	16
智能设备（物联网终端设备）	12
安全产品	7
数据库	7

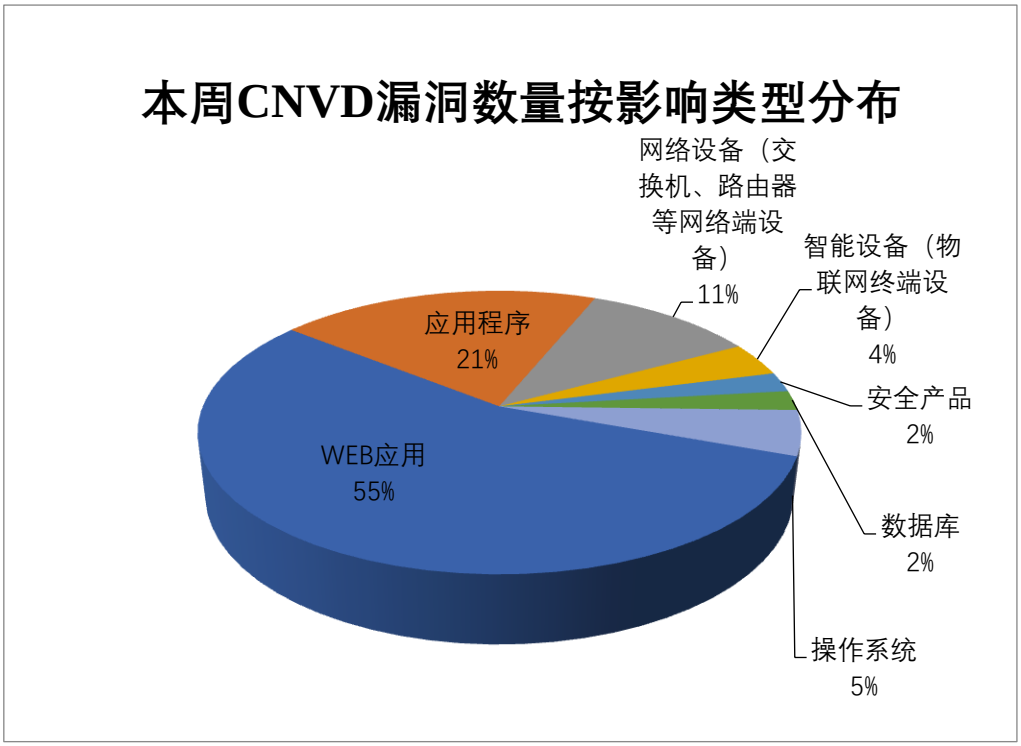

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、D-Link、IBM 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	37	12%
2	D-Link	13	4%
3	IBM	12	4%
4	Apache	11	4%
5	Cisco	11	3%
6	用友网络科技股份有限公司	10	3%
7	深圳市思迅软件股份有限公司	8	3%
8	Linux	8	3%
9	畅捷通信息技术股份有限公司	7	2%
10	其他	195	62%

本周行业漏洞收录情况

本周，CNVD 收录了 21 个电信行业漏洞，2 个移动互联网行业漏洞，1 个工控行业

漏洞（如下图所示）。其中，“Dell SmartFabric OS10 服务拒绝漏洞、Tenda FH1202 formexeCommand 方法缓冲区溢出漏洞”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/

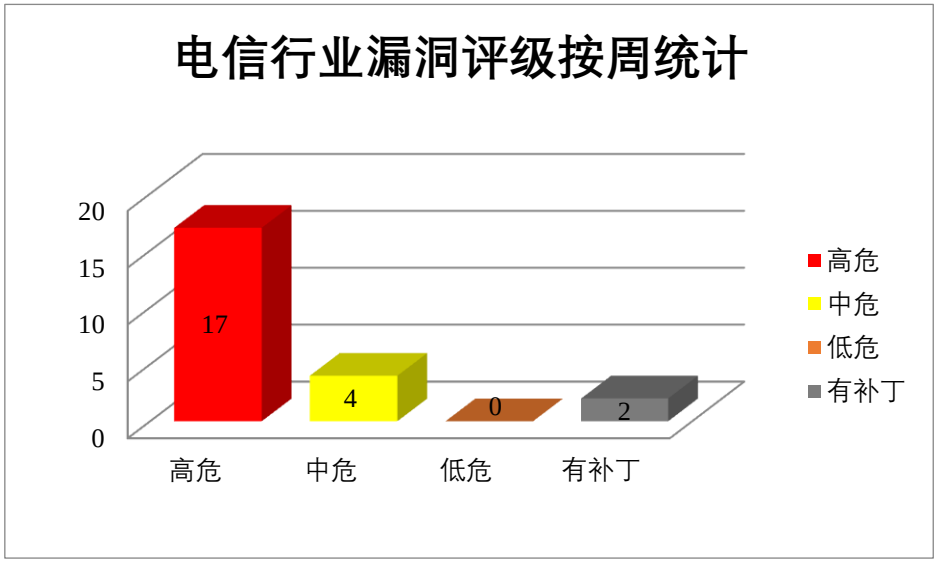

图 3 电信行业漏洞统计

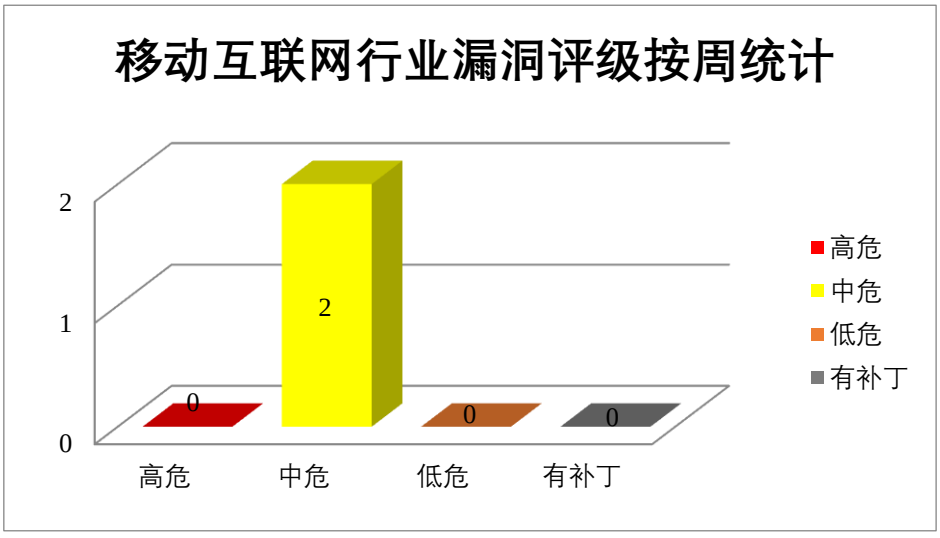

图 4 移动互联网行业漏洞统计

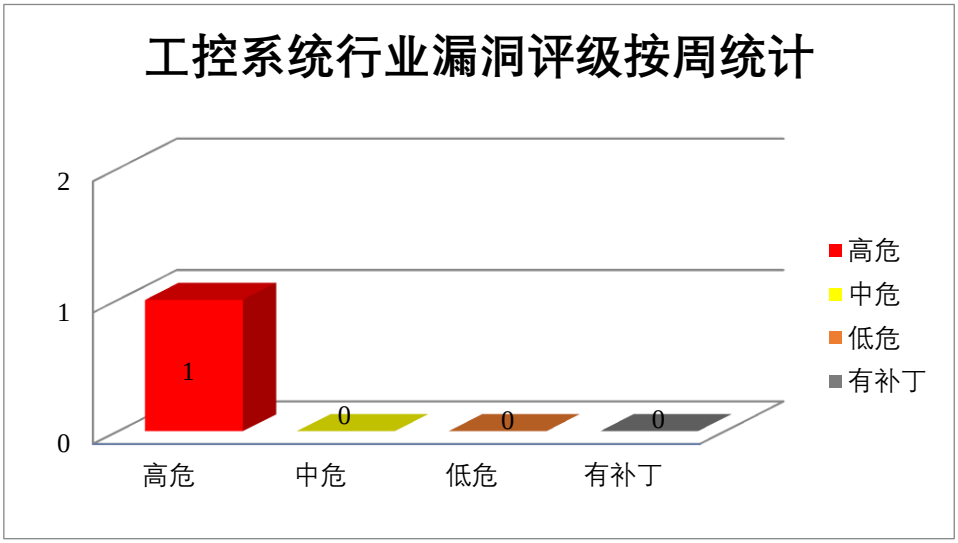

图 5 工控系统行业漏洞统计

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 MQ（IBM WebSphere MQ）是美国国际商业机器（IBM）公司的一款消息传递中间件产品。该产品主要为面向服务的体系结构（SOA）提供可靠的、经过验证的消息传递主干网。IBM MQ Operator 是美国国际商业机器（IBM）公司的一种用于管理 IBM MQ 队列管理器生命周期的工具。IBM QRadar Suite 是美国国际商业机器（IBM）公司的一款集成式的安全信息与事件管理（SIEM）解决方案，用于监控和分析组织中的网络活动以检测潜在的安全威胁。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，在某些配置下提升其权限，进行拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM MQ 拒绝服务漏洞（CNVD-2024-41243、CNVD-2024-41245）、IBM MQ 信息泄露漏洞（CNVD-2024-41242、CNVD-2024-41244）、IBM MQ 权限提升漏洞（CNVD-2024-41246）、IBM MQ Operator 信息泄露漏洞、IBM QRadar Suite 日志信息泄露漏洞（CNVD-2024-41251、CNVD-2024-41250）。其中，“IBM MQ 权限提升漏洞（CNVD-2024-41246）”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-2024-41243

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41242

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41245

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41244

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41246

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41248

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41251

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41250

2、 Cisco 产品安全漏洞

Cisco Catalyst Center（Cisco DNA Center）是美国思科（Cisco）公司的一个网络管理系统。Cisco Nexus Dashboard Fabric Controller 是美国思科（Cisco）公司的一种用于管理 Cisco NX-OS 部署的综合网络管理平台，适用于数据中心的 LAN、SAN 和 IP Fabric for Media (IPFM) 网络。Cisco IOS XE Software 是美国思科（Cisco）公司的一个操作系统。用于企业有线和无线访问，汇聚，核心和 WAN 的单一操作系统，Cisco IOS XE 降低了业务和网络的复杂性。Cisco Secure Endpoint（Cisco AMP for Endpoints）是美国思科（Cisco）公司的一套集成了静态和动态恶意软件分析以及威胁情报于一体的终端应用程序。Cisco Duo 是美国思科（Cisco）公司的一个完全托管的解决方案。提供对您的应用程序和数据的安全访问。Cisco IP Phone 是美国思科（Cisco）公司的一个硬件设备，提供通话功能的 IP 电话。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞窃取有效的用户凭据，导致设备重新加载，从而导致 DoS 情况，在受影响的设备上执行任意代码等。

CNVD 收录的相关漏洞包括：Cisco Catalyst Center 信任管理问题漏洞、Cisco Nexus Dashboard Fabric Controller 代码执行漏洞、Cisco IOS XE Software 资源管理错误漏洞（CNVD-2024-41618）、Cisco IOS XE Software 跨站请求伪造漏洞、Cisco IOS XE Software 缓冲区溢出漏洞（CNVD-2024-41616）、Cisco Secure Endpoint 缓冲区溢出漏洞、Cisco Duo 身份验证绕过漏洞、Cisco IP Phone 拒绝服务漏洞（CNVD-2024-41620）。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-2024-41614

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41613

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41618

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41617

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41616

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41622

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41621

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41620

3、 Adobe 产品安全漏洞

Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Animate 堆栈缓冲区溢出漏洞（CNVD-2024-

41254）、Adobe Animate 堆缓冲区溢出漏洞（CNVD-2024-41256）、Adobe Animate 空指针解引用漏洞（CNVD-2024-41258）、Adobe Animate 内存错误引用漏洞（CNVD-2024-41260）、Adobe Animate 整数溢出或环绕漏洞、Adobe Animate 内存错误引用漏洞（CNVD-2024-41262、CNVD-2024-41261、CNVD-2024-41263）。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-2024-41254
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41256
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41258
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41260
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41259
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41262
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41261
https://www.cnvd.org.cn/flaw/show/CNVD-2024-41263

4、 Apache 产品安全漏洞

Apache CloudStack 是美国阿帕奇（Apache）基金会的一套基础架构即服务（IaaS）云计算平台。该平台主要用于部署和管理大型虚拟机网络。Apache Lucene 是美国阿帕奇（Apache）基金会的一个免费的开源搜索引擎软件库。Apache Solr 是美国阿帕奇（Apache）基金会的一款基于 Lucene（一款全文搜索引擎）的搜索服务器。该产品支持层面搜索、垂直搜索、高亮显示搜索结果等。Apache Helix 是美国阿帕奇（Apache）基金会的一个通用集群管理框架。用于自动管理托管在节点集群上的分区、复制和分布式资源。Apache Seata 是一款开源的分布式事务解决方案，致力于在微服务架构下提供高性能和简单易用的分布式事务服务。Apache Avro 是美国阿帕奇（Apache）基金会的一个数据序列化系统。为 Apache Hadoop 提供数据序列化和数据交换服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在会话过期前访问已登出用户账户的资源，获取主机文件系统的访问权限，导致资源完整性和机密性受损、数据丢失、拒绝服务以及托管在 CloudStack 上的 KVM 基础设施的可用性问题，导致代码执行等。

CNVD 收录的相关漏洞包括：Apache CloudStack 代码问题漏洞、Apache CloudStack 输入验证错误漏洞（CNVD-2024-41660）、Apache Lucene 反序列化漏洞、Apache Solr 身份验证错误漏洞、Apache CloudStack 跨站请求伪造漏洞（CNVD-2024-41663）、Apache Helix 信任管理问题漏洞、Apache Seata 反序列化漏洞、Apache Avro 代码问题漏洞（CNVD-2024-41667）。其中，除“Apache CloudStack 代码问题漏洞”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-2024-41662

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41660

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41665

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41664

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41663

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41669

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41668

https://www.cnvd.org.cn/flaw/show/CNVD-2024-41667

5、OpenHIS SQL 注入漏洞

OpenHIS 是中国新致（OpenHIS）公司的一个基于 web 的医院管理应用程序。本周，OpenHIS 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-2024-41485

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-2024-41447	VMware vCenter Server 堆溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： VMware vCenter Server 8.0 U3d：https://support.broadcom.com/web/ecx/solutiondetails?patchId=5574 VMware vCenter Server 8.0 U2e：https://support.broadcom.com/web/ecx/solutiondetails?patchId=5531 VMware vCenter Server 7.0 U3t：
CNVD-2024-41448	Adobe Commerce 不当身份验证漏洞	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/magento/apsb24-73.html
CNVD-2024-41454	Adobe Commerce 不当输入验证漏洞（CNVD-2024-41454）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://helpx.adobe.com/security/products/magento/apsb24-73.html
CNVD-2024-41462	Adobe Commerce 跨站脚本漏洞（CNVD-2024-41462）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://helpx.adobe.com/security/products/magento/apsb24-73.html
CNVD-2024	Siemens InterMesh Subscribe	高	厂商已发布了漏洞修复程序，请及

-41572	r Devices 权限分配不正确漏洞		时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-333468.html
CNVD-2024-41575	Siemens InterMesh Subscriber Devices 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://cert-portal.siemens.com/productcert/html/ssa-333468.html
CNVD-2024-41676	Cisco Firepower Management Center SQL 注入漏洞（CNVD-2024-41676）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sqli-WFFDnNOs
CNVD-2024-41675	Mozilla Firefox 内存破坏漏洞（CNVD-2024-41675）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2024-50/
CNVD-2024-41680	Elvaco M-Bus Metering Gateway CMe3100 跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.elvaco.com/hc/en-us/articles/19039255400477-Release-notes
CNVD-2024-41688	Taquito 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://github.com/ecadlabs/taquito

小结：本周，IBM 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，在某些配置下提升其权限，进行拒绝服务攻击等。此外，Cisco、Adobe、Apache 等多款产品被披露存在多个漏洞，攻击者可利用漏洞窃取有效的用户凭据，导致设备重新加载，从而导致 DoS 情况，在受影响的设备上执行任意代码等。另外，penHIS 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。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、JEPaaS SQL 注入漏洞

验证描述

JEPaaS 是中国凯特伟业（JEPaaS）公司的一款快速开发平台。

JEPaaS v7.2.8 版本存在 SQL 注入漏洞，该漏洞源于/homePortal/loadUserMsg 的 orderSQL 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://gitee.com/ketr/jepaas-release/issues/IAPJ8H?from=project-issue

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-41484

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. Google Play 上超过 200 个恶意应用被下载了数百万次

Android 官方商店 Google Play 在一年内传播了 200 多个恶意应用程序，累计下载量接近 800 万次。

参考链接：https://www.4hou.com/posts/VW59

2. 联合健康表示，在 Change Healthcare 泄露事件中有 1 亿条数据被盗

联合健康首次确认，在 Change Healthcare 勒索软件攻击中，超过 1 亿人的个人信息和医疗数据被盗，这标志着近年来最大的医疗数据泄露事件。

参考链接：https://www.bleepingcomputer.com/news/security/unitedhealth-says-data-of-100-million-stolen-in-change-healthcare-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