国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 09 月 23 日-2024 年 09 月 29 日 **2024 年第 39 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 270 个，其中高危漏洞 121 个、中危漏洞 137 个、低危漏洞 12 个。漏洞平均分值为 6.57。本周收录的漏洞中，涉及 0day 漏洞 82 个（占 30%），其中互联网上出现“Apache Hertzbeat SQL 注入漏洞、ZZCMS 存在信息泄露漏洞（CNVD-2024-39162）”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 8664 个，与上周（12328 个）环比减少 30%。

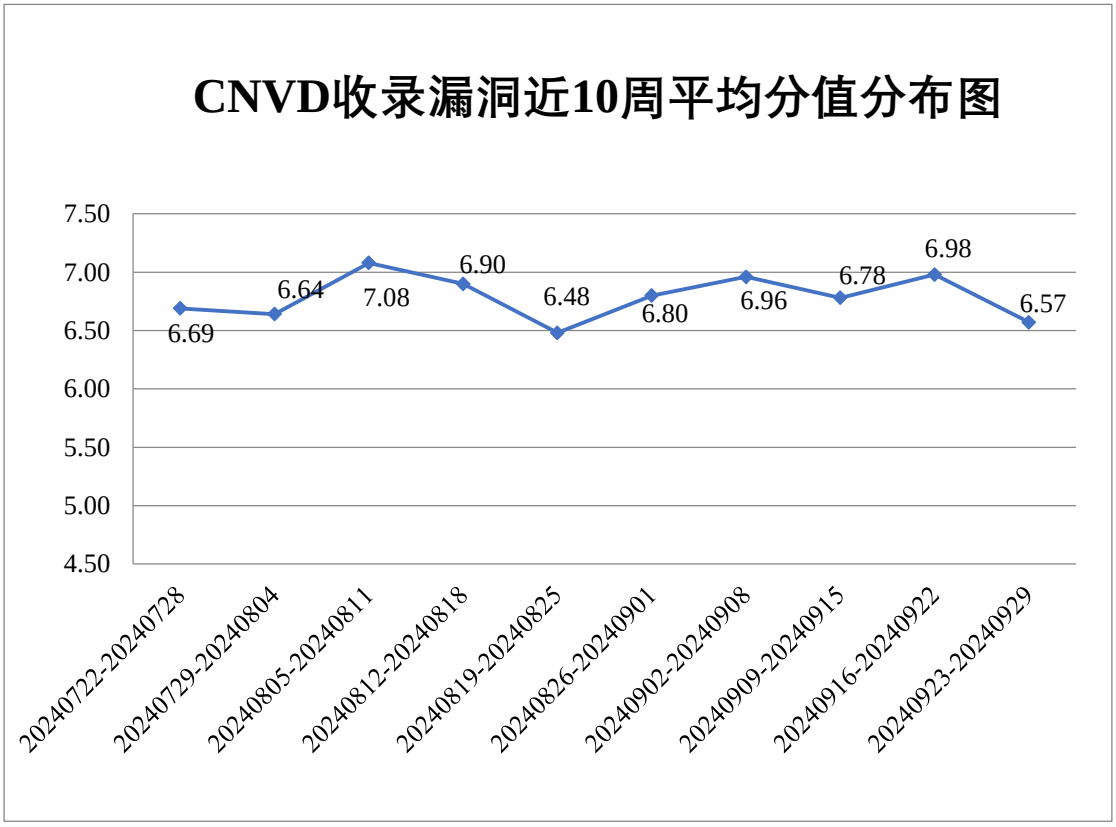

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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，CNVD 向基础电信企业通报漏洞事件 7 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 874 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 47 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 29 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、珠海新华通软件股份有限公司、重庆紫光华智科技有限公司、重庆梅安森科技股份有限公司、中新网络信息安全股份有限公司、智互联（深圳）科技有限公司、浙江兰德纵横网络技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、新天科技股份有限公司、新都（青岛）办公系统有限公司、武汉三佳医疗信息技术有限公司、武汉烽火信息集成技术有限公司、天津南大通用数据技术股份有限公司、腾讯安全应急响应中心、苏州科达科技股份有限公司、苏州汇川技术有限公司、深圳万广互联科技有限公司、深圳市中联创新自控系统有限公司、深圳市捷道智控实业有限公司、深圳市吉祥腾达科技有限公司、深圳市慧远信息科技有限公司、上海卓卓网络科技有限公司、上海辛普菲电子科技有限公司、上海桑锐电子科技股份有限公司、上海锐昉科技有限公司、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、上海博达数据通信有限公司、山东比特智能科技股份有限公司、赛蓝（广州）信息技术有限公司、润申信息科技（上海）有限公司、任子行网络技术股份有限公司、青岛和正信息技术有限公司、青岛东胜伟业软件科技有限公司、普元电力发展有限公司、普联技术有限公司、迈普通信技术股份有限公司、绿盟科技集团股份有限公司、领航未来（北京）科技有限公司、力合科技（湖南）股份有限公司、浪潮电子信息产业股份有限公司、江西铭软科技有限公司、江苏浪潮信息咨询有限公司、佳能（中国）有限公司、济南中维世纪科技有限公司、济南驰骋信息技术有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南众合百易信息技术有限公司、杭州雄伟科技开发股份有限公司、杭州三一谦成科技有限公司、汉威科技集团股份有限公司、广州图创计算机软件开发有限公司、广州同鑫科技有限公司、广州市璐华计算机科技有限公司、广东中设智控科技股份有限公司、广东保伦电子股份有限公司、福建博思软件股份有限公司、畅捷通信息技术股份有限公司、北京中科汇联信息技术有限公司、北京真内控科技有限公司、北京亿赛通科技发展有限责任公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京万户网络技术有限公司、北京容大天成科技有限公司、北京人大金仓信息技术股份有限公司、北京凯特伟业科技有限公司、北京金万维科技有限公司、北京金和网络股份有限公司、

北京北大方正电子有限公司、安美世纪（北京）科技有限公司、安徽皖通邮电股份有限公司、shopex_software 和 Emerson。

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、深信服科技股份有限公司、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。河南东方云盾信息技术有限公司、快页信息技术有限公司、贵州多彩网安科技有限公司、江苏金盾检测技术股份有限公司、北京时代新威信息技术有限公司、北京翰慧投资咨询有限公司、联想全球安全实验室、北京远禾科技有限公司、江苏正信信息安全测试有限公司及其他个人白帽子向 CNVD 提交了 12499 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 7972 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）	6475	6475
北京天融信网络安全技术有限公司	1029	0
三六零数字安全科技集团有限公司	966	966
深信服科技股份有限公司	753	0
新华三技术有限公司	701	0
上海交大	531	531
北京数字观星科技有限公司	512	0
阿里云计算有限公司	270	0
北京启明星辰信息安全技术有限公司	133	0
华为技术有限公司	102	0
恒安嘉新（北京）科技股份公司	105	0
京东科技信息技术有限公司	87	0
杭州安恒信息技术股	67	0

份有限公司		
北京升鑫网络科技有限公司（青藤云）	58	58
南京众智维信息科技有限公司	57	8
北京长亭科技有限公司	27	0
远江盛邦（北京）网络安全科技股份有限公司	15	15
长春嘉诚信息技术股份有限公司	9	9
北京云科安信科技有限公司	1	1
杭州迪普科技股份有限公司	1	1
北京神州绿盟科技有限公司	1	1
北京智游网安科技有限公司	1	1
成都卫士通信息安全技术有限公司	69	69
河南东方云盾信息技术有限公司	44	44
快页信息技术有限公司	8	8
贵州多彩网安科技有限公司	6	6
江苏金盾检测技术股份有限公司	5	5
北京时代新威信息技术有限公司	4	4
北京翰慧投资咨询有限公司	3	3
联想全球安全实验室	1	1

北京远禾科技有限公司	1	1
江苏正信信息安全测试有限公司	1	1
个人	456	456
报送总计	12499	8664

本周漏洞按类型和厂商统计

本周，CNVD 收录了 270 个漏洞。应用程序 99 个，操作系统 72 个，WEB 应用 64 个，网络设备（交换机、路由器等网络端设备）17 个，数据库 10 个，智能设备（物联网终端设备）8 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
应用程序	99
操作系统	72
WEB 应用	64
网络设备（交换机、路由器等网络端设备）	17
数据库	10
智能设备（物联网终端设备）	8

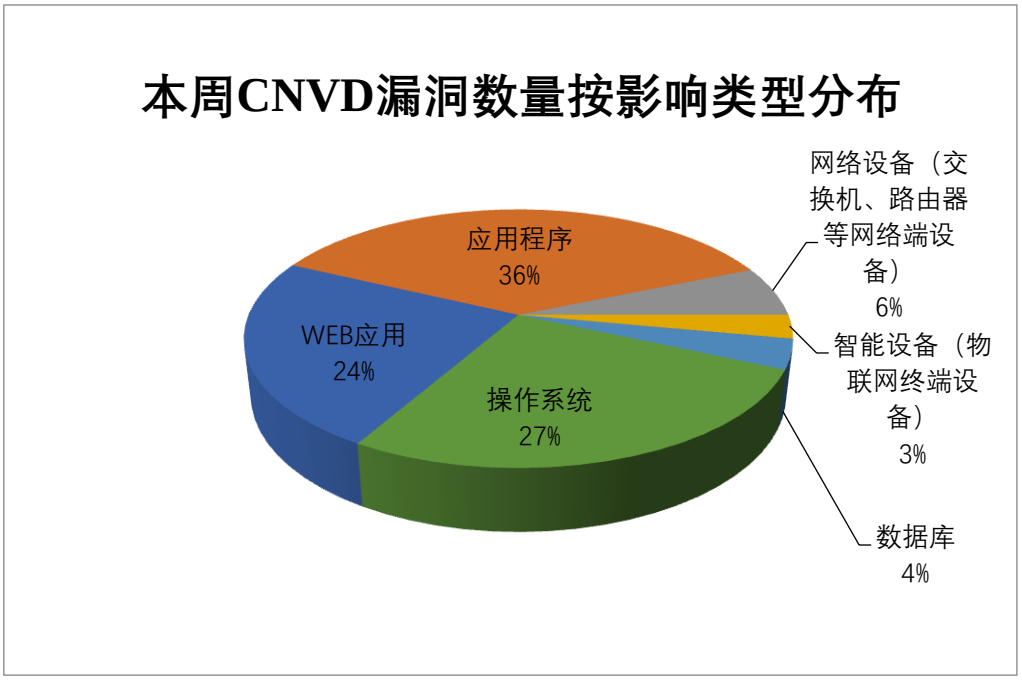

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Linux、Microsoft、DELL 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	Linux	62	23%
2	Microsoft	19	7%
3	DELL	17	7%
4	Google	15	6%
5	GTKWave	14	5%
6	Apache	14	5%
7	Wireshark	14	5%
8	用友网络科技股份有限公司	9	3%
9	Adobe	9	3%
10	其他	97	36%

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，2 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，“Dell SmartFabric OS10 命令执行漏洞、Rockwell Automation 1756-EN4 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/

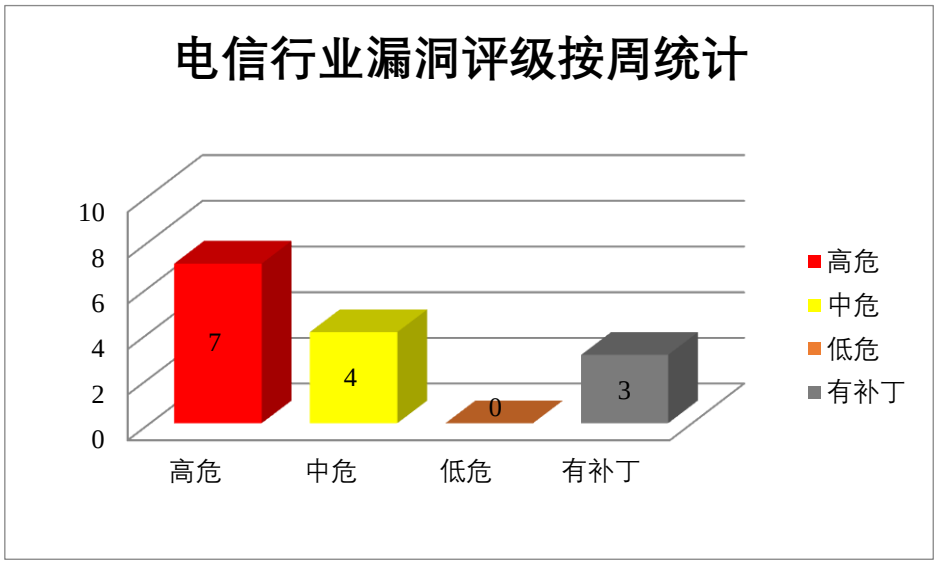

图 3 电信行业漏洞统计

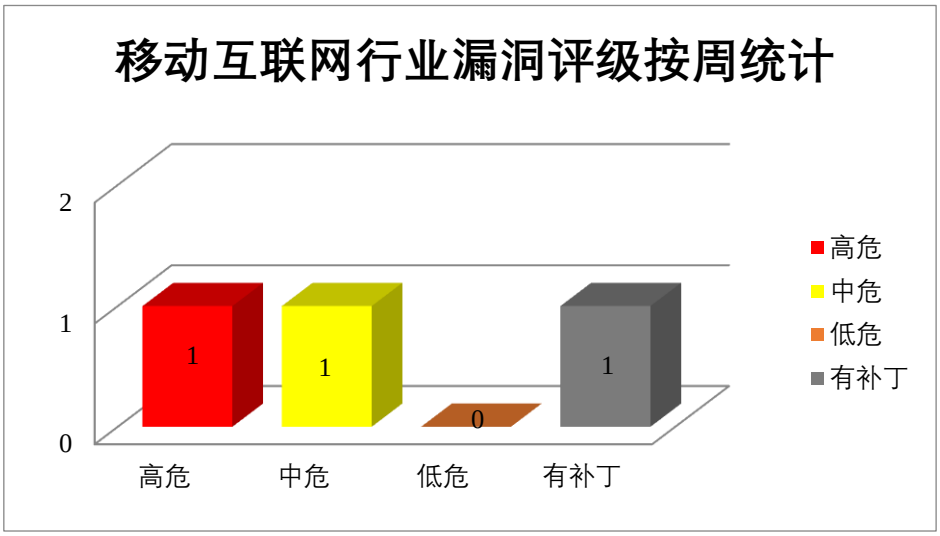

图 4 移动互联网行业漏洞统计

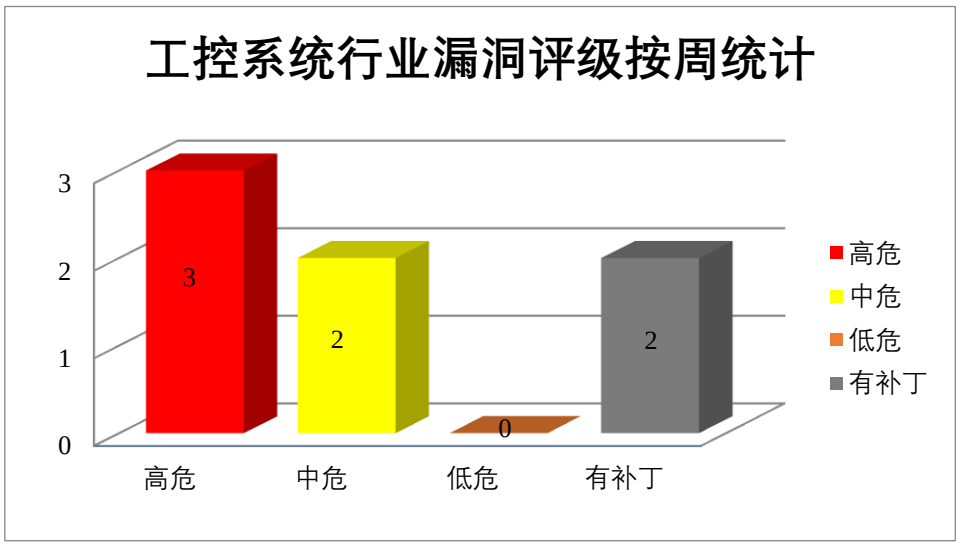

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft SQL Server 是美国微软（Microsoft）公司的一套应用在 Microsoft Windows 系统下的大型商业数据库系统。Microsoft SharePoint Server 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft SQL Server 远程代码执行漏洞（CNVD-2024-38791、CNVD-2024-38793、CNVD-2024-38797、CNVD-2024-38795）、Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2024-39521、CNVD-2024-39523、CNVD-2

024-39524、CNVD-2024-39525）。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-2024-38791
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38793
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38797
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38795
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39521
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39523
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39524
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39525

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多个漏洞，攻击者可利用漏洞绕过安全限制，通过精心制作的 HTML 页面进行越界内存访问，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome 跨站脚本漏洞（CNVD-2024-38800）、Google Chrome 越界读取漏洞（CNVD-2024-38801）、Google Chrome 越界写入漏洞（CNVD-2024-38803）、Google Chrome 内存错误引用漏洞（CNVD-2024-38802、CNVD-2024-38804）、Google Chrome 代码执行漏洞（CNVD-2024-38799、CNVD-2024-38808）、Google Chrome 安全绕过漏洞（CNVD-2024-38807）。其中，除“Google Chrome 跨站脚本漏洞（CNVD-2024-38800）、Google Chrome 安全绕过漏洞（CNVD-2024-38807）”外其余漏洞的综合评价为“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-2024-38800
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38799
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38801
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38803
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38802
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38804
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38808
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38807

3、 Apache 产品安全漏洞

Apache HertzBeat 是美国阿帕奇（Apache）公司的一个可以监控各种组件的工具。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 Allura 是美国阿帕奇

（Apache）基金会的一套开源项目托管平台。该平台支持管理源代码存储库、错误报告、维基页面和博客等。Apache StreamPipes 是美国阿帕奇（Apache）基金会的一个自助式（工业）物联网工具箱，使非技术用户能够连接、分析和探索 IIoT 数据流。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 NiFi 是一款用于构建可靠、安全的数据管道的开源工具。它支持从各种来源收集、聚合和传输数据，并提供了强大的数据处理和转换功能。Apache DolphinScheduler 是美国阿帕奇（Apache）基金会的一个分布式的基于 DAG 可视化的工作流任务调度系统。Apache Camel 是美国阿帕奇（Apache）基金会的一套开源的基于 Enterprise Integration Pattern(企业整合模式，简称 EIP)的集成框架。该框架提供企业集成模式的 Java 对象（POJO）的实现，且通过应用程序接口来配置路由和中介的规则。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在受害者的浏览器中执行 javascript 并获取有关受害者的一些敏感信息，探测服务器内网资源，通过发送恶意构造的 XML 数据来执行远程代码，执行任意代码，从而导致拒绝服务、获取敏感信息等恶意行为等。

CNVD 收录的相关漏洞包括：Apache HertzBeat 反序列化漏洞、Apache OFBiz 代码执行漏洞（CNVD-2024-39150）、Apache Allura 跨站脚本漏洞（CNVD-2024-39155）、Apache StreamPipes 服务器端请求伪造漏洞、Apache IoTDB 服务器端请求伪造漏洞、Apache NiFi 远程代码执行漏洞、Apache DolphinScheduler 输入验证错误漏洞（CNVD-2024-39158）、Apache Camel 反序列化漏洞。其中，除“Apache Allura 跨站脚本漏洞（CNVD-2024-39155）、Apache StreamPipes 服务器端请求伪造漏洞”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-2024-39149
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39150
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39155
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39154
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39153
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39160
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39158
https://www.cnvd.org.cn/flaw/show/CNVD-2024-39157

4、DELL 产品安全漏洞

Dell SmartFabric OS10 是戴尔公司推出的一款用于其交换机产品的操作系统。Dell InsightIQ 是美国戴尔（Dell）公司的一个性能监控和报告工具。Dell OpenManage Server Administrator（Dell OMSA）是美国戴尔（Dell）公司的一种软件代理。以两种方式提供全面的一对一系统管理解决方案。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。Dell BIOS 是美国戴尔（Dell）公司的一个计算机主板上小型内存芯片上的嵌入式软件。Dell NetWorker 是美国戴尔（Dell）公司的一个应用程序。提供戴尔公司的论坛讨论功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成信息泄露，导致拒绝服务，在应用程序的底层操作系统上执行任意操作系统命令，并获得特权等。

CNVD 收录的相关漏洞包括：Dell SmartFabric OS10 命令执行漏洞、Dell InsightIQ 授权问题漏洞、Dell InsightIQ 加密问题漏洞（CNVD-2024-38774）、Dell InsightIQ 访问控制错误漏洞（CNVD-2024-38773）、Dell OpenManage Server Administrator 访问控制错误漏洞、Dell PowerScale OneFS 授权问题漏洞（CNVD-2024-38779）、Dell BIOS 授权问题漏洞（CNVD-2024-38786）、Dell NetWorker 命令注入漏洞。其中，“Dell SmartFabric OS10 命令执行漏洞、Dell InsightIQ 加密问题漏洞（CNVD-2024-38774）、Dell BIOS 授权问题漏洞（CNVD-2024-38786）、Dell NetWorker 命令注入漏洞”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-2024-38776
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38775
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38774
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38773
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38780
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38779
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38786
https://www.cnvd.org.cn/flaw/show/CNVD-2024-38785

5、Tenda AC8 缓冲区溢出漏洞（CNVD-2024-39363）

Tenda AC8 是中国腾达（Tenda）公司的一款无线路由器。本周，Tenda AC8 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。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-2024-39363

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-2024-38782	Dell PowerScale OneFS 授权问题漏洞（CNVD-2024-38782）	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/000216916/dsa-2023-277-security-update-for-dell-powerscale-onefs-

			for-improper-privilege-management-vulnerability
CNVD-2024-38790	Microsoft SQL Server 信息泄露漏洞（CNVD-2024-38790）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43474
CNVD-2024-38821	Ivanti Endpoint Manager 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ivanti.com/
CNVD-2024-39036	GTKWave 整数溢出漏洞（CNVD-2024-39036）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/projects/gtkwave/files/gtkwave-3.3.118/
CNVD-2024-39043	GTKWave 内存错误引用漏洞（CNVD-2024-39043）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/projects/gtkwave/files/gtkwave-3.3.118/
CNVD-2024-39152	Apache Airflow 访问控制错误漏洞（CNVD-2024-39152）	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/2zoo8cjlwfjhbfdxfgltcm0hnc0qmc52
CNVD-2024-39159	Apache bRPC 环境问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/apache/brpc/pull/2518
CNVD-2024-39163	PublicCMS 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.publiccms.com/download.html
CNVD-2024-39252	DataEase XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/dataease/dataease/security/advisories/GHSA-4m9p-7xg6-f4mm
CNVD-2024-39271	Wireshark 拒绝服务漏洞（CNVD-2024-39271）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gitlab.com/wireshark/wireshark/-/issues/19502

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码。此外，Google、Apache、DELL 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，通过精心制作的 HTML 页面进行越界内存访问，在系统上执行任意代码等。另外，Tenda AC8 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞在系统上执行任意代码或者导致拒绝服务。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、Apache Hertzbeat SQL 注入漏洞

验证描述

Hertzbeat 是一个开源的实时监控系统。

Hertzbeat 1.6.0 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://securitylab.github.com/advisories/GHSL-2023-254_GHSL-2023-256_HertzBeat/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-39584

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. 起亚修复高危漏洞：影响大多数具备互联网连接功能汽车，攻击者可快速定位、开车门、启动引擎

绰号 specters 的网络安全专家 Neiko Rivera 于今年 6 月发现上述漏洞之后，立即通知了起亚，随后起亚高度重视，目前已经修复了这个问题。

参考链接：https://www.ithome.com/0/799/109.htm

2. 谷歌的 Gemini for Workspace 容易受到即时注入攻击

最近的一项调查显示，Google 的 Gemini for Workspace 多功能 AI 助手容易受到间接提示注入攻击。

参考链接：https://cybersecuritynews.com/gemini-workspace-prompt-injection/

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