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 15 日-2024 年 04 月 21 日　　2024 年第 16 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 610 个，其中高危漏洞 234 个、中危漏洞 362 个、低危漏洞 14 个。漏洞平均分值为 6.21。本周收录的漏洞中，涉及 0day 漏洞 548 个（占 90%），其中互联网上出现“Kirby CMS 跨站脚本漏洞、Setor Informatica SIL 跨站脚本漏洞”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 19674 个，与上周（12440 个）环比增加 58%。

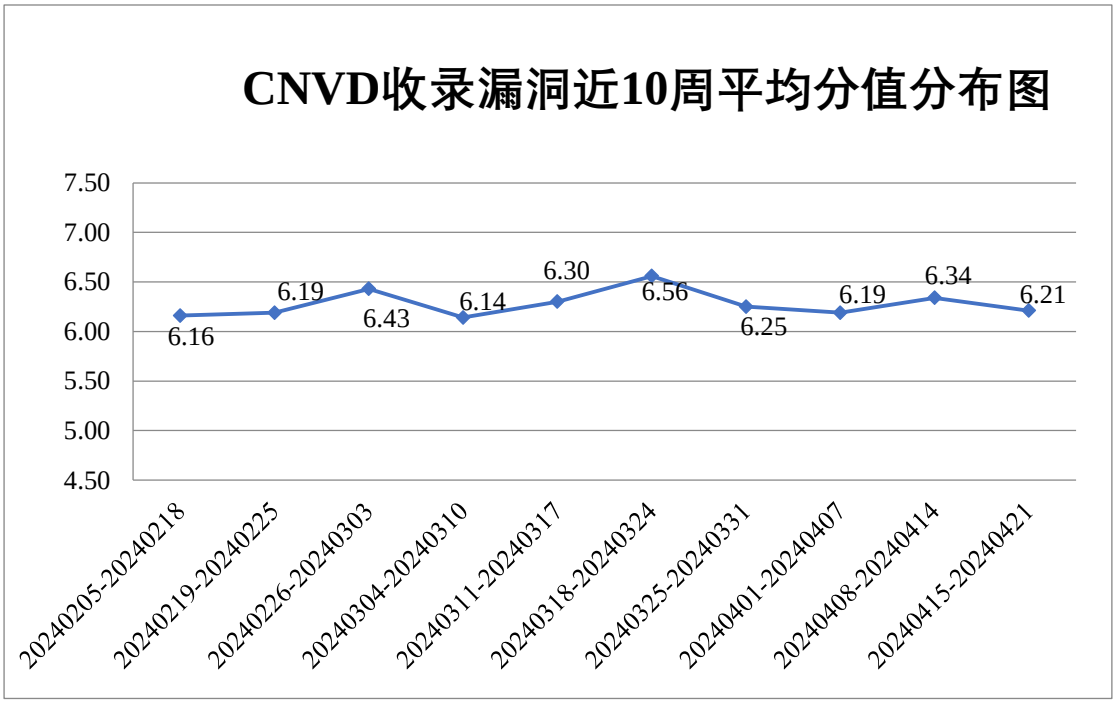

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 6 起，向基础电信

企业通报漏洞事件 9 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 666 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 58 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 14 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：

珠海奔图电子有限公司、重庆紫光华山智安科技有限公司、中林信达（北京）科技信息有限责任公司、正元智慧集团股份有限公司、浙江宇视科技有限公司、长沙友点软件科技有限公司、云南链滴科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、烟台吉安电子科技有限公司、新开普电子股份有限公司、新都（青岛）办公系统有限公司、新晨科技股份有限公司、西安众邦网络科技有限公司、西安瑞友信息技术资讯有限公司、武汉深之度科技有限公司、武汉金同方科技有限公司、万洲电气股份有限公司、统信软件技术有限公司、天维尔信息科技股份有限公司、天津天堰科技股份有限公司、宿迁鑫潮信息技术有限公司、四平市九州易通科技有限公司、神州数码控股有限公司、深圳拓安信物联股份有限公司、深圳市中电电力技术股份有限公司、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、深圳市联软科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市金证优智科技有限公司、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、深圳古瑞瓦特能源股份有限公司、深圳第五区科技有限公司、深圳奥哲网络科技有限公司、上海卓卓网络科技有限公司、上海延华智能科技（集团）股份有限公司、上海迅饶自动化科技有限公司、上海桑锐电子科技股份有限公司、上海建业信息科技股份有限公司、上海寰创通信科技股份有限公司、上海布雷德科技有限公司、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、山东山大华天软件有限公司、山东国子软件股份有限公司、厦门四信通信科技有限公司、青岛三利集团有限公司、南京科远智慧科技集团股份有限公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、江西铭软科技有限公司、江苏麦维智能科技有限公司、江苏安科瑞电器制造有限公司、济宁网众信息技术有限公司、吉翁电子（深圳）有限公司、湖南乔伦科技有限公司、湖北京山轻工机械股份有限公司、河北先河环保科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州新视窗信息技术有限公司、杭州西软信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、广州中海达卫星导航技术股份有限公司、广州图创计算机软件开发有限公司、广州斯必得电子科技有限公司、广州市保伦电子有限公司、广州恒企教育科技有限公司、广联达科技股份有限公司、广东保伦电子股份有限公司、福建科立讯通信有限公司、方正国际软件有限公司、泛微网络科技股份有限公司、东营金石软件有限公司、东莞市通天星软件科技有限公司、成都卓越远扬信息技术有限公司、北京中天慧通信息科技有限公司、北京中科商软软件有限公司、北京中成科信科技发展有限公司、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、北京小鸟科技股份有限公司、北京希瑞亚斯科技有限公司、北京通达信科科技有限公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京清科锐华软件有限公司、北京平凯星辰科技发展有限公司、北京金和网络股份有限公司、北京火绒网络科技有限公司、北京超图软件股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、暴风集团股份有限公司、安徽容知日新科技股份有限公司和安策绩效大数据有限公司。

本周，CNVD 发布了《Oracle 发布 2024 年 4 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/9941

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、天津市国瑞数码安全系统股份有限公司、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、中孚安全技术有限公司、北京中睿天下信息技术有限公司、江苏金盾检测技术股份有限公司、北京山石网科信息技术有限公司、成都久信信息技术股份有限公司、湖南泛联新安信息科技有限公司、联想集团、中资网络信息安全科技有限公司、北京天防安全科技有限公司、中国电信股份有限公司上海研究院、河南灵创电子科技有限公司、江苏省公用信息有限公司、西藏熙安信息技术有限责任公司、内蒙古洞明科技有限公司、内蒙古中叶信息技术有限责任公司、河南宝通信息安全测评有限公司、中国工商银行、北京卓识网安技术股份有限公司、山东云天安全技术有限公司、江苏晟晖信息科技有限公司、江苏锋刃信息科技有限公司、陕西青山四纪信息技术有限公司、天津市兴先道科技有限公司、广州安亿信软件科技有限公司、北京时代新威信息技术有限公司、广州万方计算机科技有限公司、成都安美勤信息技术股份有限公司、辽宁海事局、华泰证券股份有限公司、中国电信股份有限公司研究院、超聚变数字技术有限公司、北京时代新威信息技术有限公司、浙江大学控制科学与工程学院及其他个人白帽子向 CNVD 提交了 19674 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）、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 18337 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
斗象科技（漏洞盒子）	14872	14872
奇安信网神（补天平	2545	2545

台）		
新华三技术有限公司	1037	0
北京天融信网络安全技术有限公司	1024	3
上海交大	650	650
北京神州绿盟科技有限公司	404	1
天津市国瑞数码安全系统股份有限公司	383	0
三六零数字安全科技集团有限公司	270	270
北京数字观星科技有限公司	159	0
华为技术有限公司	93	0
恒安嘉新（北京）科技股份公司	92	0
北京知道创宇信息技术有限公司	80	0
北京启明星辰信息安全技术有限公司	80	6
远江盛邦（北京）网络安全科技股份有限公司	9	9
北京升鑫网络科技有限公司（青藤云）	5	5
北京安信天行科技有限公司	4	4
中国电信集团系统集成有限责任公司	1	1
北京智游网安科技有限公司	1	1
快页信息技术有限公司	60	60
河南东方云盾信息技术有限公司	35	35

中孚安全技术有限公司	21	21
北京中睿天下信息技术有限公司	13	13
江苏金盾检测技术股份有限公司	11	11
北京山石网科信息技术有限公司	11	11
成都久信信息技术股份有限公司	7	7
湖南泛联新安信息科技有限公司	6	6
联想集团	5	5
中资网络信息安全科技有限公司	5	5
北京天防安全科技有限公司	5	5
中国电信股份有限公司上海研究院	5	5
河南灵创电子科技有限公司	5	5
江苏省公用信息有限公司	4	4
西藏熙安信息技术有限责任公司	4	4
内蒙古洞明科技有限公司	4	4
内蒙古中叶信息技术有限责任公司	4	4
河南宝通信息安全测评有限公司	4	4
中国工商银行	3	3
北京卓识网安技术股份有限公司	3	3
山东云天安全技术有	3	3

限公司		
江苏晟晖信息科技有限公司	3	3
江苏锋刃信息科技有限公司	3	3
陕西青山四纪信息技术有限公司	2	2
天津市兴先道科技有限公司	2	2
广州安亿信软件科技有限公司	2	2
北京时代新威信息技术有限公司	1	1
广州万方计算机科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
辽宁海事局	1	1
华泰证券股份有限公司	1	1
中国电信股份有限公司研究院	1	1
超聚变数字技术有限公司	1	1
北京时代新威信息技术有限公司	1	1
浙江大学控制科学与工程学院	1	1
CNCERT 河北分中心	3	3
CNCERT 广西分中心	2	2
CNCERT 贵州分中心	1	1
个人	1062	1062
报送总计	23016	19674

本周漏洞按类型和厂商统计

本周，CNVD 收录了 610 个漏洞。WEB 应用 266 个，应用程序 172 个，网络设备（交换机、路由器等网络端设备）105 个，智能设备（物联网终端设备）41 个，操作系统 15 个，安全产品 7 个，数据库 4 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	266
应用程序	172
网络设备（交换机、路由器等网络端设备）	105
智能设备（物联网终端设备）	41
操作系统	15
安全产品	7
数据库	4

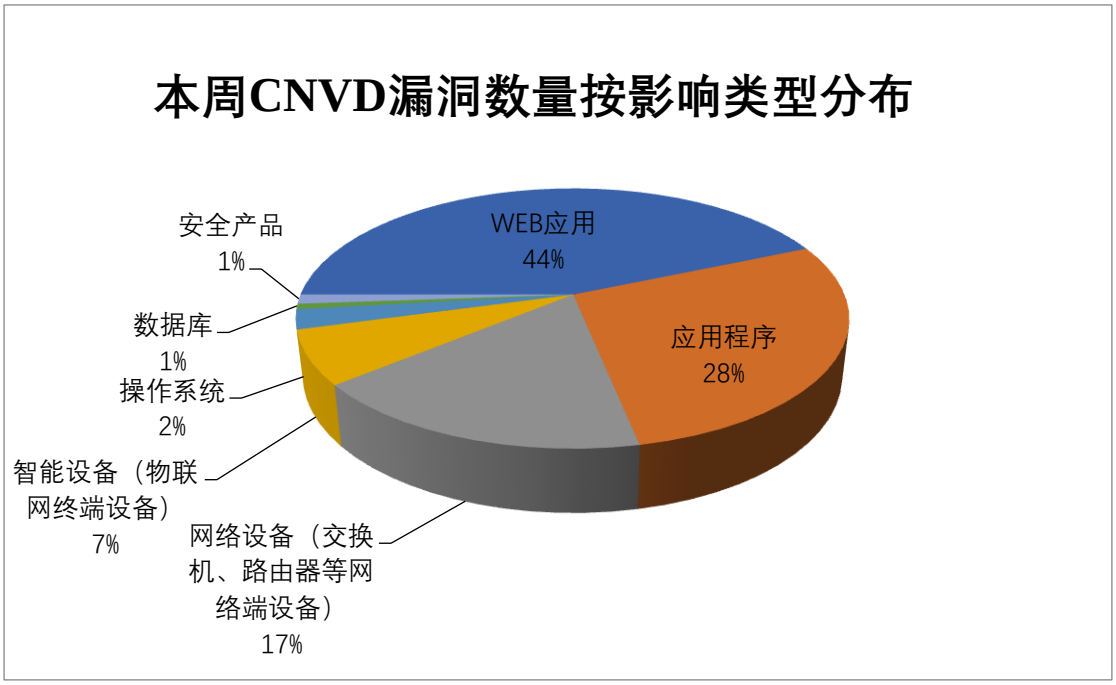

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及爱普生（中国）有限公司、北京金和网络股份有限公司、Microsoft 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	爱普生（中国）有限公司	19	3%
2	北京金和网络股份有限公司	14	2%
3	Microsoft	12	2%

4	北京星网锐捷网络技术有限公司	11	2%
5	新华三技术有限公司	10	2%
6	Adobe	10	2%
7	福建科立讯通信有限公司	10	2%
8	Apache	10	2%
9	深圳市吉祥腾达科技有限公司	9	1%
10	其他	505	82%

本周行业漏洞收录情况

本周，CNVD 收录了 37 个电信行业漏洞，62 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“Rockwell Automation Arena Simulation Software 堆缓冲区溢出漏洞、Rockwell Automation PowerFlex 527 输入验证错误漏洞”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/

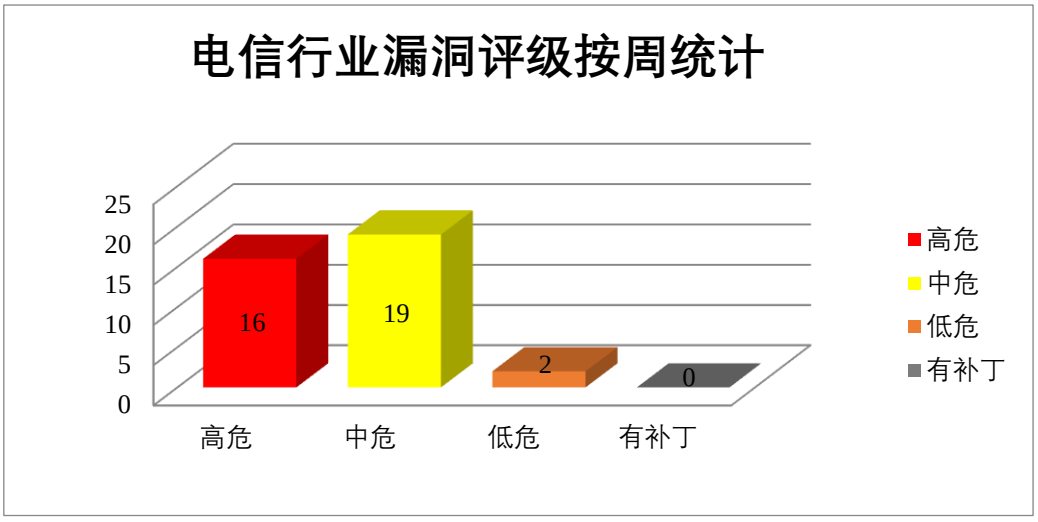

图 3 电信行业漏洞统计

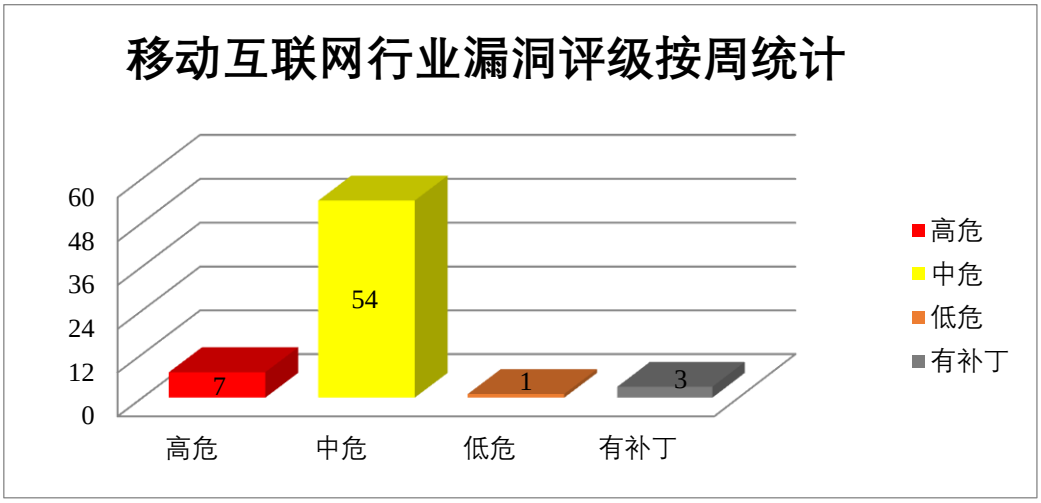

图 4 移动互联网行业漏洞统计

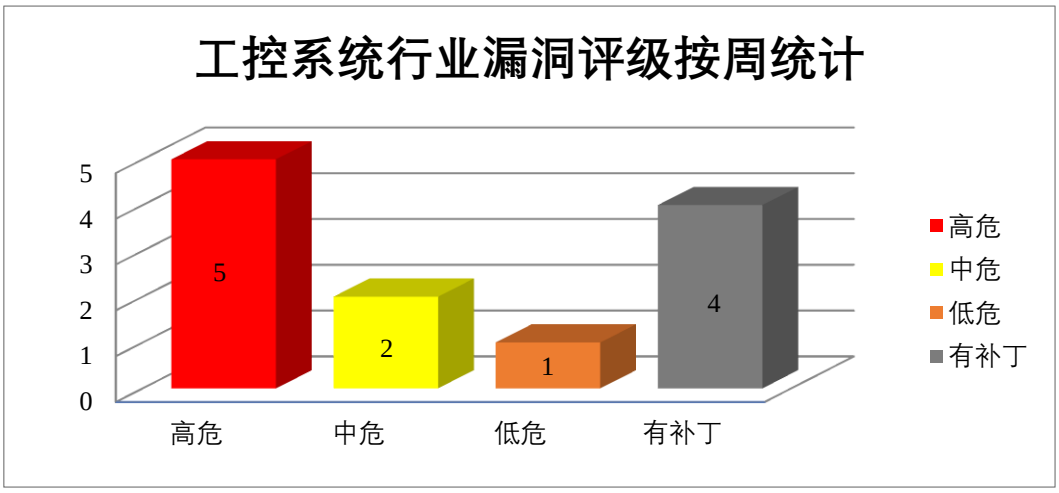

图 5 工控系统行业漏洞统计

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 Zeppelin 是美国阿帕奇（Apache）基金会的一款基于 Web 的开源笔记本应用程序。该程序支持交互式数据分析和协作文档。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替换 Apache Zeppelin 中的现有注释，绕过身份验证，通过发送特制请求，导致拒绝服务条件等。

CNVD 收录的相关漏洞包括：Apache Zeppelin 输入验证错误漏洞（CNVD-2024-17935、CNVD-2024-17934、CNVD-2024-17937、CNVD-2024-17936）、Apache Zeppelin 代码执行漏洞、Apache Zeppelin 安全绕过漏洞、Apache Zeppelin 代码注入漏洞（CNVD-2024-17938、CNVD-2024-17940）。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-2024-17935
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17934
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17933
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17932
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17938
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17937
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17936
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17940

2、 Apple 产品安全漏洞

Apple iOS 和 Apple iPadOS 都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Apple macOS Ventura 是一个桌面操作系统。Apple macos 是一套操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感信息，导致拒绝服务，能够使用内核权限执行任意代码等。

CNVD 收录的相关漏洞包括：Apple iOS and iPadOS 代码执行漏洞、Apple macOS Ventura 竞争条件问题漏洞、Apple macOS Ventura 拒绝服务漏洞、Apple macOS Ventura 资源管理错误漏洞（CNVD-2024-17855）、Apple 多款产品缓冲区溢出漏洞、Apple macos 缓冲区溢出漏洞（CNVD-2024-17858）、Apple macOS 安全特征问题漏洞（CNVD-2024-17859）、Apple iOS 和 Apple iPadOS 缓冲区溢出漏洞。其中，“Apple iOS and iPadOS 代码执行漏洞、Apple 多款产品缓冲区溢出漏洞、Apple iOS 和 Apple iPadOS 缓冲区溢出漏洞”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-2024-17852
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17853
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17854
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17855
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17856
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17858
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17859
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17860

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。本周，上述产品被披露存在跨站脚本漏洞，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。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-17888、CNVD-2024-17892、CNVD-2024-17891、CNVD-2024-17890、CNVD-2024-17896、CNVD-2024-17895、CNVD-2024-17894、CNVD-2024-17893）。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-2024-17888
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17892
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17891
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17890
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17896
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17895
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17894
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17893

4、Microsoft 产品安全漏洞

Microsoft Edge 是美国微软（Microsoft）公司的一款 Windows 10 之后版本系统附带的 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，进行欺骗攻击，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Edge (Chromium-based)欺骗漏洞（CNVD-2024-17969、CNVD-2024-17971）、Microsoft Edge (Chromium-based)安全功能绕过漏洞（CNVD-2024-17970、CNVD-2024-17978）、Microsoft Edge for Android (Chromium-based)信息泄露漏洞、Microsoft Edge (Chromium-based)信息泄露漏洞（CNVD-2024-17973、CNVD-2024-17975）、Microsoft Edge (Chromium-based)远程代码执行漏洞（CNVD-2024-17976）。其中，“Microsoft Edge (Chromium-based)信息泄露漏洞（CNVD-2024-17975）、Microsoft Edge (Chromium-based)远程代码执行漏洞（CNVD-2024-17976）”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-2024-17969
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17970
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17971
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17972
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17973
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17975
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17976
https://www.cnvd.org.cn/flaw/show/CNVD-2024-17978

5、Tenda W20E 栈缓冲区溢出漏洞

Tenda W20E 是一款由 Tenda 公司开发的无线路由器，主要用于提供无线网络连接和管理功能。本周，Tenda W20E 被披露存在栈缓冲区溢出漏洞。攻击者可利用该漏洞执行任意代码。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-2024-18609

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-2024-17852	Apple iOS and iPadOS 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT213938
CNVD-2024-17856	Apple 多款产品缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT213721
CNVD-2024-17940	Apache Zeppelin 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://zeppelin.apache.org/
CNVD-2024-17975	Microsoft Edge (Chromium-based)信息泄露漏洞（CNVD-2024-17975）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26192
CNVD-2024-17976	Microsoft Edge (Chromium-based)远程代码执行漏洞（CNVD-2024-17976）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21399
CNVD-2024-18059	IBM WebSphere Application Server Liberty 资源管理错误漏洞（CNVD-2024-18059）	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/7145365
CNVD-2024-18334	Rockwell Automation Arena Simulation Software 未初始化指针访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://download.rockwellautomation.com/esd/download.aspx?downloadid=RAid1141475
CNVD-2024-18333	Rockwell Automation Arena Simulation Software 免费后使用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://download.rockwellautomation.com/esd/download.aspx?downloadi

			d=RAid1141475
CNVD-2024-18332	Rockwell Automation Arena Simulation Software 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://download.rockwellautomation.com/esd/download.aspx?downloadid=RAid1141475
CNVD-2024-18335	Rockwell Automation PowerFlex 527 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.rockwellautomation.com/en-us/support/advisory.SD1664.html

小结：本周，Apache 产品被披露存在多个漏洞，攻击者可利用漏洞通过替换 Apache Zeppelin 中的现有注释，绕过身份验证，通过发送特制请求，导致拒绝服务条件等。此外，Apple、Adobe、Microsoft 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，通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML，在系统上执行任意代码，导致拒绝服务等。另外，Tenda W20E 被披露存在栈缓冲区溢出漏洞。攻击者可利用漏洞执行任意代码。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、Setor Informatica SIL 跨站脚本漏洞

验证描述

Setor Informatica SIL 是 Setor Informatica 公司的一种用于连接医学实验室的解决方案。

Setor Informatica SIL 3.1 版本存在跨站脚本漏洞，该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过 hmessage 参数运行任意代码。

验证信息

POC 链接：https://github.com/ELIZEUOPAIN/CVE-2024-24035/tree/main

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-18357

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. Palo Alto Networks 披露 PAN-OS 防火墙漏洞细节

该漏洞被追踪为 CVE-2024-3400，CVSS 评分 10 分，具体涉及 PAN-OS 10.2、PAN-OS 11.0 和 PAN-OS 11.1 防火墙版本软件中的两个缺陷。

参考链接：https://www.freebuf.com/news/398643.html

2. PuTTY SSH 工具发布更新，修复漏洞：私钥可被窃取

攻击者只需要访问几十条已签名消息和公钥，就能从中恢复私钥，后续就可以伪造签名，并在未经授权的情况下访问服务器。

参考链接：https://www.ithome.com/0/762/546.htm

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