国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 08 月 19 日-2024 年 08 月 25 日 **2024 年第 34 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 308 个，其中高危漏洞 152 个、中危漏洞 138 个、低危漏洞 18 个。漏洞平均分值为 6.48。本周收录的漏洞中，涉及 0day 漏洞 223 个（占 72%），其中互联网上出现“TOTOLINK X5000R setModifyVpnUser 方法命令注入漏洞、ZZCMS 任意文件读取漏洞”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 44226 个，与上周（27939 个）环比增加 58%。

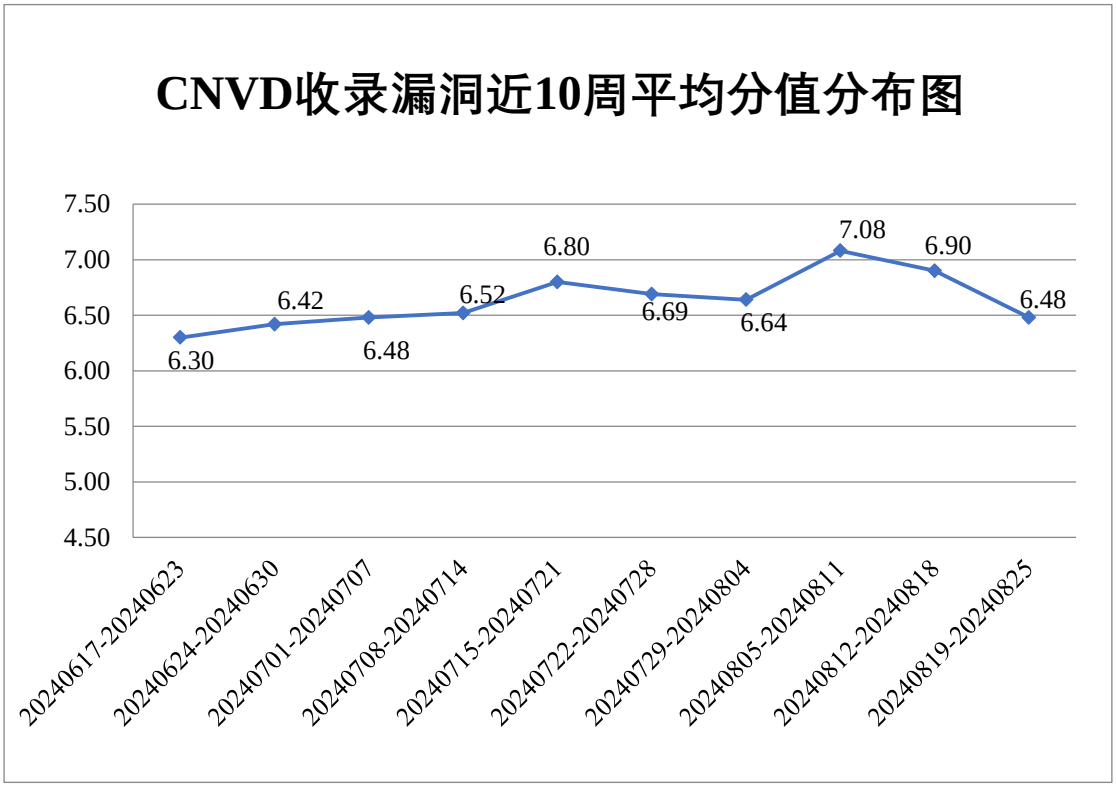

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 2 起，向基础电信企业通报漏洞事件 2 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 601 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 33 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：

紫光集团有限公司、中译语通科技股份有限公司、智互联（深圳）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、新天科技股份有限公司、武汉达梦数据库有限公司、天津卓朗科技发展有限公司、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、松下电器（中国）有限公司、四川迅睿云软件开发有限公司、四川天健世纪科技有限公司、神州数码控股有限公司、深圳市深科特信息技术有限公司、深圳市吉祥腾达科技有限公司、深圳市东宝信息技术有限公司、上海卓卓网络科技有限公司、上海异工同智信息科技有限公司、上海移远通信技术股份有限公司、上海桑锐电子科技股份有限公司、上海锐昉科技有限公司、上海金慧软件有限公司、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、山东比特智能科技股份有限公司、厦门科拓通讯技术股份有限公司、麒麟软件有限公司、力合科技（湖南）股份有限公司、蓝网科技股份有限公司、蓝鸽集团有限公司、科大讯飞股份有限公司、杭州三汇信息工程有限公司、杭州品联科技有限公司、杭州吉拉科技有限公司、杭州海康威视数字技术股份有限公司、广东中设智控科技股份有限公司、广东飞企互联科技股份有限公司、东华软件股份公司、成都同飞科技有限责任公司、畅捷通信息技术股份有限公司、北京致远互联软件股份有限公司、北京真视通科技股份有限公司、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、北京通达信科科技有限公司、北京神州视翰科技有限公司、北京人大金仓信息技术股份有限公司、北京朗新天霁软件技术有限公司、北京金和网络股份有限公司、北京奥泰瑞格科技有限公司、奥琦玮信息科技（北京）有限公司和安歌科技（集团）股份有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、北京神州绿盟科技有限公司、北京天融信网络安全技术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、信息产业信息安全测评中心、成都久信信息技术股份有限公司、快页信息技术有限公司、北京山石网科信息技术有限公司、苏州棱镜七彩信息科技有限公司、中资网络信息安全科技有限公司、上海观安信息技术股份有限公司、江苏极元信息技术有限公司、重庆都会

信息科技有限公司、南方电网数字电网集团信息通信科技有限公司、北京翰慧投资咨询有限公司、北京远禾科技有限公司、北京天下信安技术有限公司、安徽希客安全技术服务有限公司、博智安全科技股份有限公司、江西中和证信息安全技术有限公司、安徽天行网安信息安全技术有限公司、中国人民财产保险股份有限公司、北京卓识网安技术股份有限公司、江苏软测信息科技有限公司及其他个人白帽子向 CNVD 提交了 44226 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 43110 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）	26043	26043
奇安信网神（补天平台）	15622	15622
三六零数字安全科技集团有限公司	1159	1159
新华三技术有限公司	942	0
安天科技集团股份有限公司	453	0
深信服科技股份有限公司	418	20
北京神州绿盟科技有限公司	335	0
上海交大	286	286
北京天融信网络安全技术有限公司	250	1
京东科技信息技术有限公司	119	0
北京启明星辰信息安全技术有限公司	98	35
恒安嘉新（北京）科技股份公司	83	0
中国电信集团系统集成有限责任公司	23	23
北京知道创宇信息技术有限公司	21	2

北京长亭科技有限公司	19	1
杭州安恒信息技术股份有限公司	12	4
北京安信天行科技有限公司	11	11
远江盛邦（北京）网络安全科技股份有限公司	10	10
南京众智维信息科技有限公司	4	4
华为技术有限公司	3	3
河南东方云盾信息技术有限公司	31	31
信息产业信息安全测评中心	14	14
成都久信信息技术股份有限公司	13	13
快页信息技术有限公司	11	11
北京山石网科信息技术有限公司	8	8
苏州棱镜七彩信息科技有限公司	8	8
中资网络信息安全科技有限公司	7	7
上海观安信息技术股份有限公司	5	5
江苏极元信息技术有限公司	3	3
重庆都会信息科技有限公司	2	2
南方电网数字电网集团信息通信科技有限公司	2	2

北京翰慧投资咨询有限公司	2	2
北京远禾科技有限公司	2	2
北京天下信安技术有限公司	1	1
安徽希客安全技术服务有限公司	1	1
博智安全科技股份有限公司	1	1
江西中和证信息安全技术有限公司	1	1
安徽天行网安信息安全技术有限公司	1	1
中国人民财产保险股份有限公司	1	1
北京卓识网安技术股份有限公司	1	1
江苏软测信息科技有限公司	1	1
CNCERT 贵州分中心	6	6
CNCERT 浙江分中心	2	2
CNCERT 宁夏分中心	2	2
个人	876	876
报送总计	46913	44226

本周漏洞按类型和厂商统计

本周，CNVD 收录了 308 个漏洞。WEB 应用 154 个，应用程序 74 个，网络设备（交换机、路由器等网络端设备）39 个，智能设备（物联网终端设备）25 个，操作系统 8 个，数据库 6 个，安全产品 2 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	154
应用程序	74
网络设备（交换机、路由器等网络端设备）	39

智能设备（物联网终端设备）	25
操作系统	8
数据库	6
安全产品	2

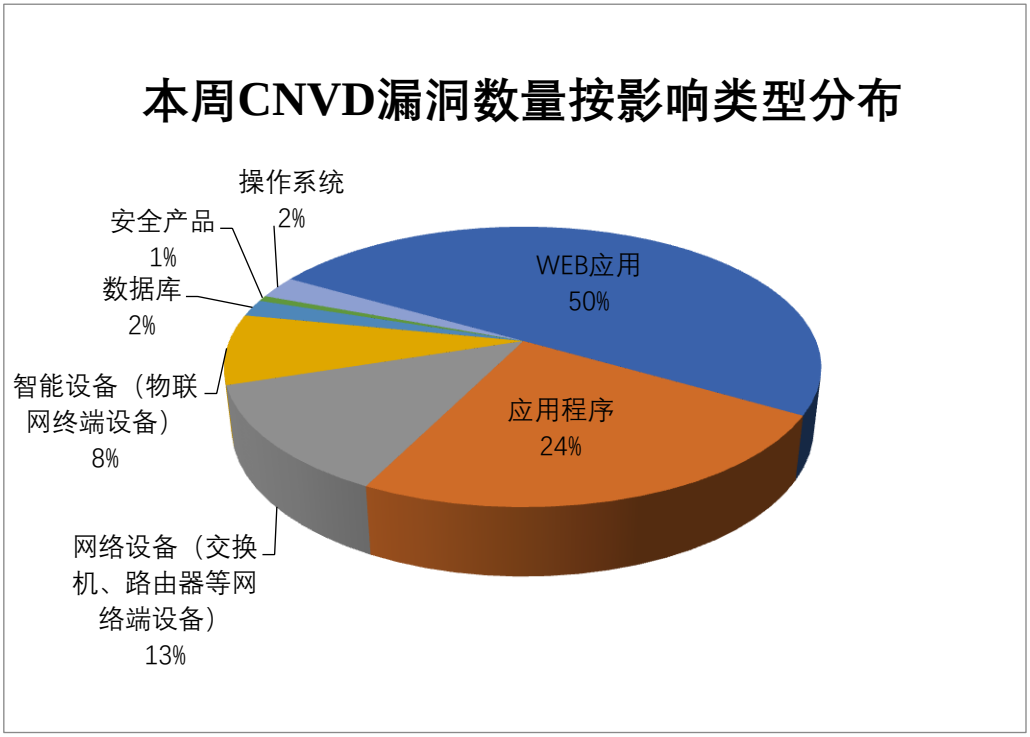

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、TOTOLINK、Google 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	33	11%
2	TOTOLINK	15	5%
3	Google	13	4%
4	SAP	12	4%
5	北京神州视翰科技有限公司	12	4%
6	Apache	12	4%
7	用友网络科技股份有限公司	8	3%
8	畅捷通信息技术股份有限公司	7	2%
9	北京人大金仓信息技术股份有限公司	6	2%
10	其他	190	61%

本周行业漏洞收录情况

本周，CNVD 收录了 32 个电信行业漏洞，15 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，“Tenda FH1202 form_fast_setting_wifi_set 方法缓冲区溢出漏洞、Huawei HarmonyOS 和 EMUI 拒绝服务漏洞（CNVD-2024-36099）”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/

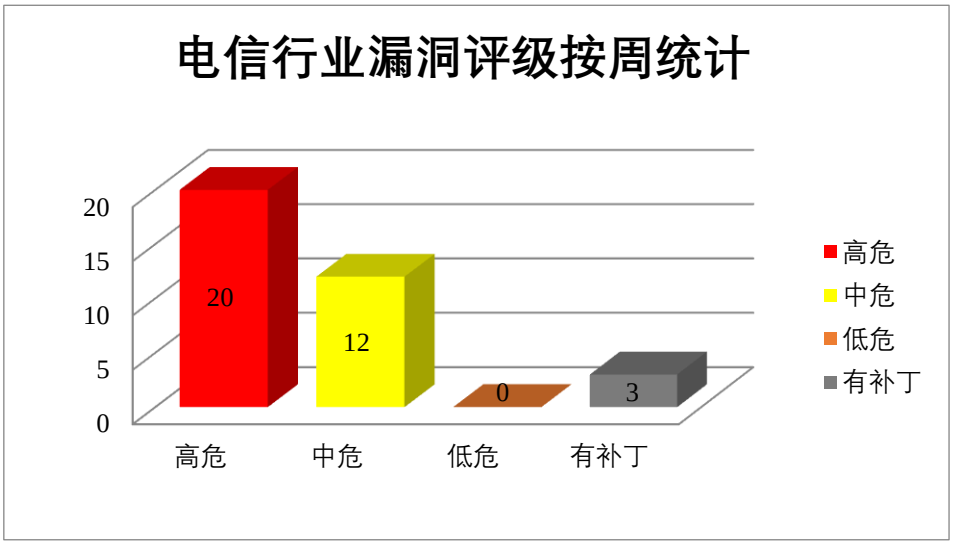

图 3 电信行业漏洞统计

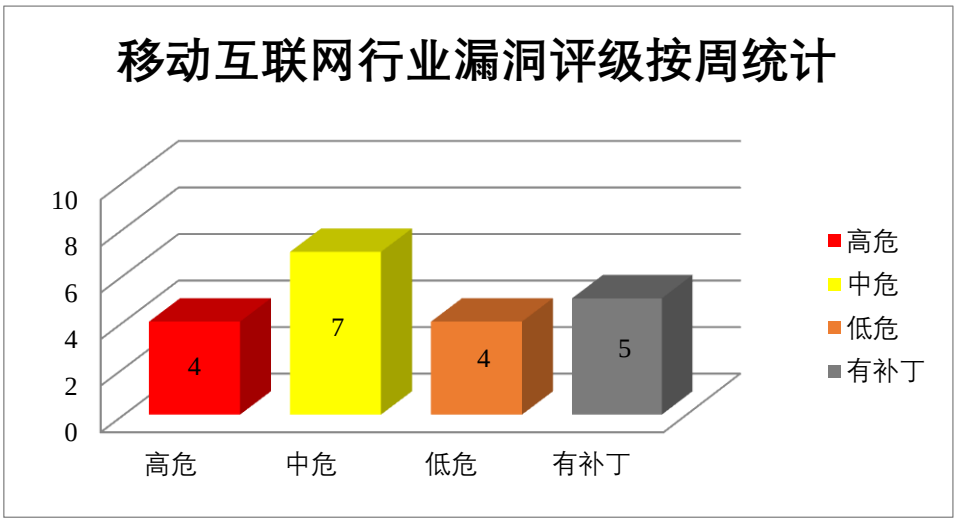

图 4 移动互联网行业漏洞统计

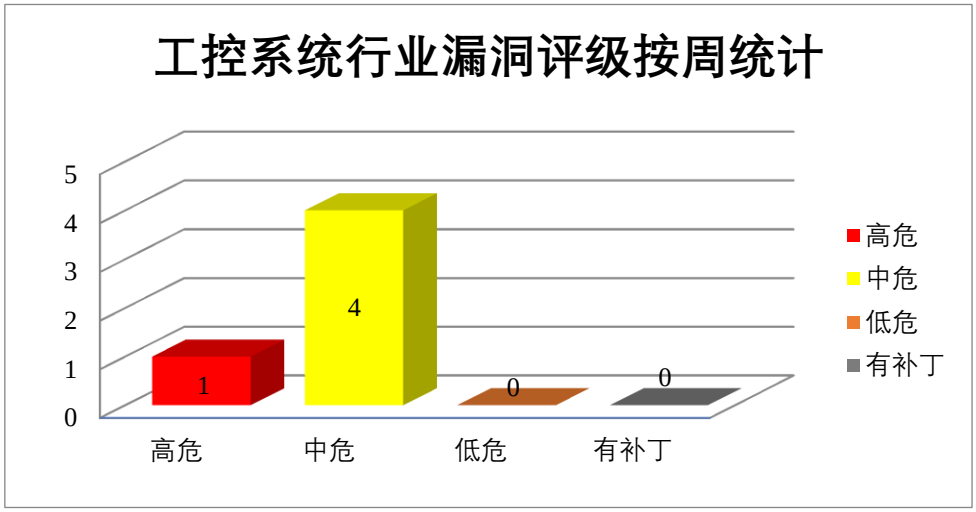

图 5 工控系统行业漏洞统计

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、 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，在系统上执行任意代码或导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Chrome Audio 模块内存错误引用漏洞、Google Chrome Browser UI 模块内存错误引用漏洞、Google Chrome PDFium 模块内存错误引用漏洞、Google Chrome Tab Strip 模块缓冲区溢出漏洞、Google Chrome V8 模块内存错误引用漏洞、Google Chrome 安全绕过漏洞（CNVD-2024-36090、CNVD-2024-36091）、Google Chrome 代码执行漏洞（CNVD-2024-36093）。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-2024-36085

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36086

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36087

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36088

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36089

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36090

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36091

https://www.cnvd.org.cn/flaw/show/CNVD-2024-36093

2、 Adobe 产品安全漏洞

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe Dimension 是美国奥多比（Adobe）公司的是一套 2D 和 3D 合成设计工具。Adobe InDesign 是美国奥多比（Adobe）公司的一套排版编辑应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码，或者导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Adobe Bridge 越界写入漏洞（CNVD-2024-35982、CNVD-2024-35983）、Adobe Dimension 越界写入漏洞（CNVD-2024-35995）、Adobe Dimension 内存错误引用漏洞（CNVD-2024-35998）、Adobe InDesign 越界读取漏洞（CNVD-2024-36305）、Adobe InDesign 越界写入漏洞（CNVD-2024-36304、CNVD-2024-36303、CNVD-2024-36306）。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-2024-35982
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35983
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35995
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35998
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36305
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36304
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36303
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36306

3、SAP 产品安全漏洞

SAP CRM 是德国思爱普（SAP）公司的一个客户关系管理系统。SAP My Travel Requests 是美国思爱普（SAP）公司的一个交易应用程序。SAP Enable Now Manager 是德国思爱普（SAP）公司的中央内容管理和协作平台。SAP BusinessObjects BI Platform 是德国思爱普（SAP）公司的用于数据报告、可视化和共享的集中套件。SAP NetWeaver Application Server 是德国思爱普（SAP）公司的一款应用程序服务器。SAP CRM 是德国思爱普（SAP）公司的一个客户关系管理系统。SAP Commerce 是德国思爱普（SAP）公司的一套基于云的电子商务平台。该产支持销售管理、营销管理、订单管理和运营管理等。SAP Business Workflow 是德国思爱普（SAP）公司的用于执行业务流程的关键组件，它允许用户设计、实施和管理业务流程，确保流程的合规性，并通过自动化减少手动操作的需要。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，执行执行任意代码，导致权限升级等。

CNVD 收录的相关漏洞包括：SAP CRM 信息泄露漏洞、SAP My Travel Requests 授权问题漏洞、SAP Enable Now Manager 授权问题漏洞、SAP BusinessObjects BI Platform 反序列化漏洞、SAP NetWeaver Application Server 文件上传漏洞、SAP CRM 授权问题漏洞、SAP Commerce 授权问题漏洞（CNVD-2024-36346）、SAP Business Wor

kflow 信息泄露漏洞。其中，“SAP BusinessObjects BI Platform 反序列化漏洞、SAP NetWeaver Application Server 文件上传漏洞”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-2024-35653
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35656
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35655
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35660
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35658
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36348
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36346
https://www.cnvd.org.cn/flaw/show/CNVD-2024-36345

4、Apache 产品安全漏洞

Apache Answer 是美国阿帕奇（Apache）基金会的一个社区平台。Apache MINA SSHD 是美国阿帕奇（Apache）基金会的一个纯 Java 库，支持客户端和服务器端的 SSH 协议。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 Answer 是美国阿帕奇（Apache）基金会的一个社区平台。Apache Linkis 是美国阿帕奇（Apache）基金会的一款中间件产品，可以在上层应用和底层数据引擎之间建立起有效的连接。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 Traffic Server 是美国阿帕奇（Apache）基金会的一套可扩展的 HTTP 代理和缓存服务器。Apache SeaTunnel 是美国阿帕奇（Apache）基金会的一个简单易用的数据集成框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞伪造任何令牌来登录任何用户，远程代码执行，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Apache Answer 安全绕过漏洞（CNVD-2024-35661）、Apache MINA SSHD 安全绕过漏洞、Apache DolphinScheduler 输入验证错误漏洞（NVD-C-2024-618180）、Apache Answer 安全绕过漏洞、Apache Linkis 权限提升漏洞、Apache InLong 代码注入漏洞（CNVD-2024-35666）、Apache Traffic Server 输入验证错误漏洞（CNVD-2024-35671）、Apache SeaTunnel 认证绕过漏洞。其中，除“Apache MINA SSHD 安全绕过漏洞”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-2024-35661
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35664
https://www.cnvd.org.cn/flaw/show/CNVD-2024-35663

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35662

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35668

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35666

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35671

https://www.cnvd.org.cn/flaw/show/CNVD-2024-35669

5、Tenda AX1806 缓冲区溢出漏洞（CNVD-2024-35918）

Tenda AX1806 是中国腾达（Tenda）公司的一个 WiFi6 无线路由器。本周，Tenda AX1806 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过特制的输入导致拒绝服务。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-2024-35918

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-2024-36029	Adobe Illustrator 越界写入漏洞（CNVD-2024-36029）	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/illustrator/apsb24-45.html
CNVD-2024-35926	北京亿赛通科技发展有限责任公司亿赛通电子文档安全管理系统存在 SQL 注入漏洞（CNVD-2024-35926）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://update.nsfocus.com/update/listCdgDetail/v/cdg820-old https://update.nsfocus.com/update/listCdgDetail/v/new-system5.6.2
CNVD-2024-36032	Adobe Substance 3D Designer 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://helpx.adobe.com/security/products/substance3d_designer/apsb24-67.html
CNVD-2024-35962	用友网络科技股份有限公司 NC Cloud 存在 SQL 注入漏洞（CNVD-2024-35962）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.yonyou.com/#/noticeInfo?id=432
CNVD-2024-36031	Adobe Illustrator 不当输入验证漏洞	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/illustrator/apsb24-45.html
CNVD-2024-36084	泛微网络科技股份有限公司 e-cology 产品 H2 组件远程命令执行漏洞	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://www.weaver.com.cn/cs/securit

			y/edm20240815_kdielfrovkewpiiuyrtewtw.html
CNVD-2024-36101	Tenda FH1202 form_fast_setting_wifi_set 方法缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/
CNVD-2024-36308	Adobe InDesign 整数溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/indesign/apsb24-56.html
CNVD-2024-36112	北京星网锐捷网络技术有限公司 DDI1000 存在命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ruijie.com.cn/
CNVD-2024-36299	Adobe InDesign 缓冲区溢出漏洞（CNVD-2024-36299）	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/indesign/apsb24-56.html

小结：本周，Google 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，在系统上执行任意代码或导致应用程序崩溃。此外，Adobe、SAP、Apache 等多款产品被披露存在多个漏洞，攻击者可利用漏洞伪造任何令牌来登录任何用户，获取敏感信息，在系统上执行任意代码，导致拒绝服务等。另外，Tenda AX1806 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过特制的输入导致拒绝服务。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、 TOTOLINK X5000R setModifyVpnUser 方法命令注入漏洞

验证描述

TOTOLINK X5000R 是中国吉翁电子（TOTOLINK）公司的一个路由器。

TOTOLINK X5000R setModifyVpnUser 方法存在命令注入漏洞，攻击者可利用该漏洞执行任意命令。

验证信息

POC 链接：https://github.com/HouseFuzz/reports/blob/main/totolink/x5000r/setModifyVpnUser/setModifyVpnUser.md

参考链接：https://nvd.nist.gov/vuln/detail/CVE-2024-42744

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. Litespeed 曝出高速缓存漏洞，数百万 WordPress 网站面临安全威胁

近日，有研究人员在插件的用户模拟功能中发现了未经身份验证的权限升级漏洞（CVE-2024-28000），该漏洞是由 LiteSpeed Cache 6.3.0.1 及以下版本中的弱散列检查引起的。这个漏洞可能会让攻击者在创建恶意管理员账户后接管数百万个网站。

参考链接：https://www.freebuf.com/news/409193.html

2. 适用于 macOS 的多个微软应用程序发现库注入漏洞，用户数据安全受威胁

根据 Cisco Talos 的最新研究，macOS 上的八个微软应用程序容易受到库注入攻击，有可能让攻击者劫持应用程序的权限并泄露敏感数据。受影响的微软应用程序包括 Microsoft Teams、Outlook、PowerPoint 和 Word 等流行服务，共有八个 CVE 编号。

参考链接：https://www.freebuf.com/news/409025.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