SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

让每个用户的数字化更简单、更安全

网络安全半月刊

（2025 年 5 月下）

深信服科技股份有限公司

2025 年 6 月 4 日

■ 信息来源

国家信息安全漏洞共享平台（CNVD）

国家互联网应急响应中心（CNCERT/CC）

深信服千里目安全技术中心

深信服云端威胁对抗指挥中心

深信服安全 BG一全球安全运营中心

互联网新闻资讯

■ 编辑/审阅

深信服千里目安全技术中心

深信服安全 BG一全球安全运营中心

深信服品牌营销部

说明

本半月刊涵盖 2025 年 5 月份(5.15-5.31)深信服团队发现的新增安全漏洞，并将此期间国际国内发生的热点安全事件、最新政策法规动态等进行总结整理与解读，希望与广大用户及时分享网络安全现状及最新热点资讯，欢迎讨论指正。文档内引用了部分互联网已公开的数据信息，均已在文档里标明出处。

本期可以关注 VMware vCenter 认证后命令执行漏洞，CNVD 发布了 5 月漏洞详情，建议受影响用户及时更新升级至最新版本。如参加国家级实战攻防演练的用户，请留意及时做好更新。

本期网络安全政策法律动态信息：

国内政策法规：

1、六部门联合公布《国家网络身份认证公共服务管理办法》

2、中国人民银行发布《中国人民银行业务领域网络安全事件报告管理办法》

3、全国网安标委发布《网络安全标准实践指南—个人信息保护合规审计要求》

4、国家数据局局长：统筹数据发展和安全，持续推进数据要素市场化价值化

国际政策法规：

1、美国国家标准与技术研究院（NIST）发布《网络安全白皮书 41 号》

2、英国国防部成立新网络战司令部，投资 10 亿英镑提升数字战能力

深信服安全团队拥有优秀的安全技术专家，可扫码关注深信服千里目安全技术中心微信公众号，第一时间了解最新的安全事件、威胁漏洞情报等。

深信服千里目安全技术中心公众号二维码

目 录

一、网络安全政策法律动态

（一）国内政策法规

1、六部门联合公布《国家网络身份认证公共服务管理办法》

5 月 23 日，公安部、国家互联网信息办公室、民政部、文化和旅游部、国家卫生健康委员会、国家广播电视总局等六部门联合公布《国家网络身份认证公共服务管理办法》（以下简称《管理办法》），自 2025 年 7 月 15 日起施行。

公安部、国家互联网信息办公室等部门建设了国家网上身份认证基础设施，向社会提供国家网络身份认证公共服务，满足人民群众在数字化、网络化、智能化条件下安全、便捷证明个人身份的需求，有效保护个人信息安全，促进数字经济高质量发展。目前，国家网络身份认证公共服务已在部分互联网平台和政务服务、教育考试、文化旅游、医疗卫生、邮政寄递、交通出行等行业领域开展了试点应用。为进一步规范国家网络身份认证公共服务的使用范围、使用方式、使用场景、使用原则，明确相关方的权利义务、职责任务、法律责任，公安部、国家互联网信息办公室等六部门制定了《管理办法》。

原文链接：

国家网络身份认证公共服务管理办法_中央网络安全和信息化委员会办公室

权威 FAQ丨公安部有关部门负责人就《国家网络身份认证公共服务管理办法》答记者问

2、中国人民银行发布《中国人民银行业务领域网络安全事件报告管理办法》

5 月 23 日，为进一步规范涉及货币信贷、宏观审慎、跨境人民币、银行间市场、金融业综合统计、支付清算、人民币发行流通、经理国库、征信和信用评级、反洗钱等中国人民银行业务领域网络安全事件报告管理，指导督促金融从业

机构依法依规报告中国人民银行业务领域网络安全事件（以下简称网络安全事件），中国人民银行发布《中国人民银行业务领域网络安全事件报告管理办法》（中国人民银行令〔2025〕第 4 号，以下简称《办法》），自 2025 年 8 月 1 日起施行。

下一步，中国人民银行将组织实施好《办法》，指导金融从业机构及时、准确报告网络安全事件，降低网络安全事件造成的损失和危害，筑牢金融网络安全防线。

原文链接：

中国人民银行令〔2025〕第 4 号(中国人民银行业务领域网络安全事件报告管理办法)

3、全国网安标委发布《网络安全标准实践指南—个人信息保护合规审计要求》

5 月 26 日，根据《中华人民共和国个人信息保护法》《个人信息保护合规审计管理办法》等法律法规要求，为指导个人信息保护合规审计活动，保护个人信息权益，全国网络安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南——个人信息保护合规审计要求》。

本《实践指南》提出了个人信息保护合规审计原则，规定了个人信息保护合规审计的总体要求、实施流程、内容和方法，适用于个人信息处理者和专业机构开展个人信息保护合规审计活动。

原文链接：

关于发布《网络安全标准实践指南——个人信息保护合规审计要求》的通知

4、国家数据局局长：统筹数据发展和安全，持续推进数据要素市场化价值化

5 月 17 日，国家数据局党组书记、局长刘烈宏在浙江温州召开的“瓯江论数 数安未来”2025 数据安全发展大会上发表致辞。

致辞中表示，希望各方在确保数据安全基础上，加快打通公共数据共享开放壁垒，推动公共数据与企业数据资源融合应用，力争打赢服务“两个主战场”的

攻坚战。同时，还要鼓励引导各类企业在做好运用数据要素降本增效、提质升级的同时，加力让沉睡的企业数据“供出来、用起来”，更好服务产业链、生态链上的大中小企业，助力传统产业深度转型，促进人工智能等未来产业快速发展，切实将海量数据资源转化为发展新质生产力的新优势。

原文链接：

国家数据局局长刘烈宏：统筹数据发展和安全，持续推进数据要素市场化价值化

（二）国际政策法规

1、美国国家标准与技术研究院（NIST）发布《网络安全白皮书 41 号》

5 月 29 日消息，近日美国国家标准与技术研究院（NIST）发布了《网络安全白皮书 41 号》(CSWP41)，提出了一种名为“可能被利用漏洞”(Likely Exploited Vulnerabilities，简称 LEV）的新型安全指标，用于衡量软件和硬件漏洞被实际利用的可能性。

该指标旨在弥补现有漏洞管理工具的不足，特别是在当前广泛使用的漏洞预测评分系统（EPSS）和已知被利用漏洞列表（KEV）存在局限性的背景下。

原文链接：

NIST 发布“漏洞预测指标”，大幅提升漏洞管理能力

2、英国国防部成立新网络战司令部，投资 10 亿英镑提升数字战能力

5 月 30 日消息，英国国防部(MoD)宣布成立新的网络与电磁司令部，并投资

10 亿英镑增强武装部队的数字战争能力。该司令部负责保护英国军事网络免受日益增长的网络攻击，并与此前成立的国家网络部队(NCF)协调进行攻击性网络行动。

此举是英国政府将网络行动置于英国防御战略前沿计划的一部分，作为其战略防御评估(SDR)的组成部分。SDR 建议英国国防部应在 2027 年前交付数字目标网。此外，英国国防部还将加快招募网络安全专业人才。据悉，英国在过去两年中经历了 9 万次敌对国家的网络入侵。

原文链接：

UK MoD Launches New Cyber Warfare Command - Infosecurity Magazine

二、安全热点时事资讯

（一）国内安全事件

1、因违反网络安全、数据安全管理规定等，多家银行机构被罚款

时间：5 月下旬

概况：

5 月 14 日，中国人民银行三门峡市分行发布的行政处罚信息显示，三门峡农商银行因“未按规定履行客户身份识别义务；违反信用信息采集、提供、查询及相关管理规定；违反网络安全管理规定”等 6 项违法行为，被警告，并被罚款 55.1 万元。

5 月 19 日，中国人民银行商丘市分行发布的行政处罚信息显示，睢县农村信用合作联社因“未按照规定报送可疑交易报告；违反信用信息采集、提供、查询及相关管理规定；违反网络安全管理规定；违反数据安全管理规定”等 8 项违法行为，被警告，并被罚款 64.4 万元。

据显示，近期已有多家银行收到网络安全相关罚单，涉及大行和中小银行。

安全警示与建议：（适配银行等金融机构）

- 合规管理常态化：严格落实《数据安全管理办法》，建立数据分类分级制度，定期开展内部审计，确保账户管理、清算流程等符合监管要求。
- 加强网络安全防护：采用零信任架构，对客户敏感数据实施加密存储，通过安全 GPT、XDR 等系统实现跨平台安全联动检测。
- 加强员工安全意识培训：针对反洗钱、反假货币等业务开展专项培训，避免因操作疏漏引发风险。

原文链接：

罚单 | 因违反网络安全管理规定等，这家银行被罚

罚单 | 因违反网络安全、数据安全管理规定等，这家农信联社被罚

2、郑州某公司系统因网络安全问题被境外势力上传恶意标语，被行政处罚

时间：5 月 23 日

概况：

【网信郑州】公众号发文称，某公司未履行网络安全保护义务，引发网络安全事件，依据《网络安全法》责令整改，给予警告，并罚款三万元。

经调查，该公司在网络安全方面意识淡薄，未建立健全网络安全等级保护制度，其网络办公系统存在部分未选择记录日志功能、防火墙未禁用高危端口、未对账户进行重命名、未及时修复漏洞隐患、未对数据库加密处理、应用程序版本过低等 9 个问题，境外不法分子利用该系统存在的漏洞，上传恶意标语，引发网络安全事件，造成严重恶劣影响。

安全防御建议：（适配所有企业单位）

网络安全的基础防护工作是抵御网络攻击的第一道防线，是构建可信数字环境的基石。此次事件的发生再次为企业敲响警钟，安全无小事，失守往往源于细节的疏漏。企业应从人、制度、技术三个层面全面加强网络安全管理，将“安全优先”的理念融入企业文化和业务流程之中，切实提升整体的网络安全防护能力。

- 漏洞全生命周期管理：建立 “扫描 - 修复 - 验证” 闭环流程，尤其关注开源组件（如 ComfyUI）的漏洞通告，及时部署官方补丁 411。

- 监控与响应能力建设：通过流量分析、日志审计等技术手段，实现对异常行为的实时预警，缩短攻击响应时间至分钟级。
- 供应链安全审查：对第三方服务提供商进行严格的安全评估，避免因供应商漏洞导致供应链攻击。

原文链接：

某公司违反《网络安全法》被郑州市网信办行政处罚

由郑州某公司系统被境外势力上传恶意标语看基础安全

3、境外黑客利用 ComfyUI 漏洞对我实施网络攻击

时间：5 月 27 日

概况：

国家网络安全通报中心发布消息：目前已有境外黑客组织利用 ComfyUI 漏洞对我网络资产实施网络攻击，伺机窃取重要敏感数据。ComfyUI 是一款 AI 绘图工具，专为图像生成任务设计，通过将深度学习模型的工作流程简化为图形化节点，使用户操作更加直观和易于理解。

近期，北京市网络与信息安全信息通报中心发现，ComfyUI 存在任意文件读取、远程代码执行等多个历史高危漏洞（CVE-2024-10099、CVE-2024-21574、CVE-2024-21575、CVE-2024-21576、CVE-2024-21577），攻击者可利用上述漏洞实施远程代码执行攻击，获取服务器权限，进而窃取系统数据。

安全防护建议：

官方提醒，建议相关用户在确保安全的前提下，及时下载升级官方补丁堵塞漏洞，同时做好类似人工智能大模型应用的安全加固，确保网络和数据安全，发现遭攻击情况第一时间向当地公安机关报告。

原文链接：

官方提醒：境外黑客利用 ComfyUI 漏洞对我实施网络攻击

（二）国际安全事件

1、维多利亚的秘密、卡地亚等知名时尚品牌接连遭遇黑客攻击

时间：5 月 24 日

概况：

过去一个月，时尚品牌频频成为黑客目标。继法国奢侈品牌迪奥（Dior）和卡地亚（Cartier）以及德国运动品牌阿迪达斯（Adidas）披露数据泄露事件后，近日美国时尚零售巨头维多利亚的秘密（Victoria's Secret）也因 5 月 24 日的网络安全事件推迟了 2025 年第一季度财报发布。

当日维多利亚的秘密遭遇网络安全攻击，迫使公司在 5 月 26 日关闭了企业系统、部分门店服务和电子商务网站作为预防措施。公司后在新闻发布会上表示，网站已于 5 月 29 日恢复，但企业系统的全面恢复仍在进行中。

此次事件影响了部分门店的有限功能，尽管大多数已恢复正常。由于系统恢复进程，员工无法访问支持 2025 年第一季度（截至 5 月 3 日）财报发布所需的关键系统和信息，公司因此推迟了原定的财报发布和电话会议网络直播。维多利亚的秘密已聘请外部专家评估事件影响，但尚未公开事件的具体性质，外界猜测可能涉及勒索软件攻击。

安全防御建议：（对于时尚零售等行业）

时尚零售行业正面临前所未有的网络安全挑战。高端的品牌和客户更需要高端的网络安全，随着黑客手段日益复杂，奢侈品牌和零售巨头需进一步投入资源，提升系统安全性，以保护客户数据和企业运营。网络安全已成为时尚行业的新“品牌力”。

- 客户数据精细化管理：采用差分隐私技术对消费数据进行脱敏处理，限制高权限账号的访问范围。

- 加强第三方风险管控：对电商平台、支付网关等合作伙伴进行定期安全审计，签订数据保护协议并明确违约责任。
- 舆情与危机管理：建立数据泄露快速响应机制，72 小时内完成内部调查并向监管部门报备，同时通过官方渠道向客户致歉并提供补救措施。
- 消费者应警惕可疑邮件或通信，避免点击不明链接或提供个人信息。

原文链接：

维多利亚的秘密、卡地亚等知名时尚品牌接连遭遇黑客攻击

2、新斯科舍电力公司遭勒索软件攻击 28 万用户数据泄露

时间：5 月 27 日

概况：

加拿大新斯科舍电力公司证实遭遇一起复杂的勒索软件攻击，约 28 万客户的敏感信息被窃。该公司表示，在拒绝支付赎金后，攻击者已开始公开发布窃取的数据。

此次网络攻击最初于 2025 年 4 月 25 日被发现，当时 IT 安全团队注意到部分网络段和业务应用服务器存在未授权访问。然而后续调查显示，系统的初始入侵可能早在 3 月 19 日就已发生，这意味着攻击者在未被发现的情况下潜伏了约五周时间。

目前该公司已与环联(TransUnion)合作，通过 TransUnion myTrueIdentity®为受影响客户提供为期两年的免费信用监测服务。同时提醒客户警惕利用泄露数据进行的社交工程和钓鱼攻击。

安全防护建议：（适配关键基础设施行业）

该事件凸显了关键基础设施面临日益复杂的勒索软件威胁，也警示能源行业必须加强网络安全建设。

- 加强关键基础设施防护：采用 “隔离 + 冗余” 架构，对电力调度、客户数据等核心系统实施物理隔离，同时建立异地灾备中心。

- 健全数据备份策略：定期进行离线备份，并测试恢复流程的有效性，确保在遭受攻击时可快速回滚数据。
- 开展应急响应演练：每季度开展模拟勒索软件攻击的实战演练，明确各部门职责，缩短从发现攻击到启动预案的时间。

原文链接：

【安全圈】新斯科舍电力公司遭勒索软件攻击 28 万用户数据泄露

3、华硕路由器遭新型僵尸网络入侵，固件更新也无法清除持久化攻击

时间：2025 年 5 月

概况：

网络安全研究人员发现一种名为 AyySSHush 的新型隐蔽僵尸网络正在全球范围内针对华硕路由器发起攻击。该僵尸网络最早由 GreyNoise 在 2025 年 3 月发现，随后被 Censys 持续追踪，其通过滥用路由器合法功能建立长期控制，使得检测和修复变得极其困难。

截至 2025 年 5 月 28 日，Censys 已发现 4,504 台受感染的华硕路由器，受害者主要分布在美国、瑞典、台湾地区、新加坡和香港地区。HINET、MobileOne、HKT、Telia、Comcast 和 Charter 等住宅 ISP 用户的设备受影响最为严重。

研究人员特别提醒："即使是主动升级路由器固件的用户也可能在不知情的情况下持续遭受入侵。"这种针对住宅网络基础设施的攻击策略，使得僵尸网络能够利用住宅 IP 相对可信的特性，有效规避基于 IP 的检测系统，非常适合用于构建分布式代理基础设施和匿名恶意活动。

安全团队可采取以下防护措施：

- 使用 Censys 提供的查询工具，通过检测 TCP 53282 端口和 ASUS 品牌设备识别暴露的路由器；
- 监控未经授权的 SSH 密钥；
- 对路由器进行系统重装；

- 在禁用持久性配置同步功能后再考虑硬件重置。

原文链接：

华硕路由器遭新型僵尸网络入侵，固件更新也无法清除持久化攻击

三、安全风险通告

VMware vCenter 认证后命令执行漏洞(CVE-2025-41225)

漏洞名称 ：VMware vCenter 认证后命令执行漏洞(CVE-2025-41225)

漏洞描述：2025 年 5 月 21 日，深瞳漏洞实验室监测到一则 VMware-vCenter 组件存在命令执行漏洞的信息，漏洞编号：CVE-2025-41225，漏洞威胁等级：高危。vCenter 服务器存在一个命令执行漏洞，**具有创建，修改 alarms 或运行 scripts 权限的用户可以利用该漏洞执行任意命令，导致服务器失陷**。

漏洞编号：CVE-2025-41225，漏洞威胁等级：**高危**。

组件介绍：

VMware vCenter 是一种高级服务器管理软件，它提供了一个集中式平台来控制 vSphere 环境以实现跨混合云的可见性。

影响范围：

目前受影响的 VMware vCenter 版本：

vCenter Server 7.0 < 7.0 U3v

vCenter Server 8.0 < 8.0 U3e **利用条件：**

1、用户认证：需要用户认证

2、前置条件：默认配置

3、触发方式：远程

<综合评定利用难度>：容易，具有一定权限的用户可以执行任意命令。

<综合评定威胁等级>：高危，能造成任意命令执行。

官方解决方案：

官方已发布最新版本修复该漏洞，建议受影响用户将 VMware vCenter 更新到以下版本：

vCenter Server 7.0 U3v

vCenter Server 8.0 U3e

其他低版本 vCenter Server 同样受该漏洞影响，建议低版本用户更新 7.0 或 8.0 补丁。

链接如下：

https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/release-notes/vcenter-server-update-and-patch-release-notes/vsphere-vcenter-server-80u3e-release-notes.html

https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/7-0/release-notes/vcenter-server-update-and-patch-releases/vsphere-vcenter-server-70u3v-release-notes.html

深信服解决方案：

漏洞安全监测

对 VMware-vCenter 的主动检测，可批量检出业务场景中该事件的受影响资产情况，相关产品如下：

【深信服云镜 YJ】已发布资产检测方案，指纹 ID:0010456。

【深信服漏洞评估工具 TSS】已发布资产检测方案，指纹 ID:0010456。

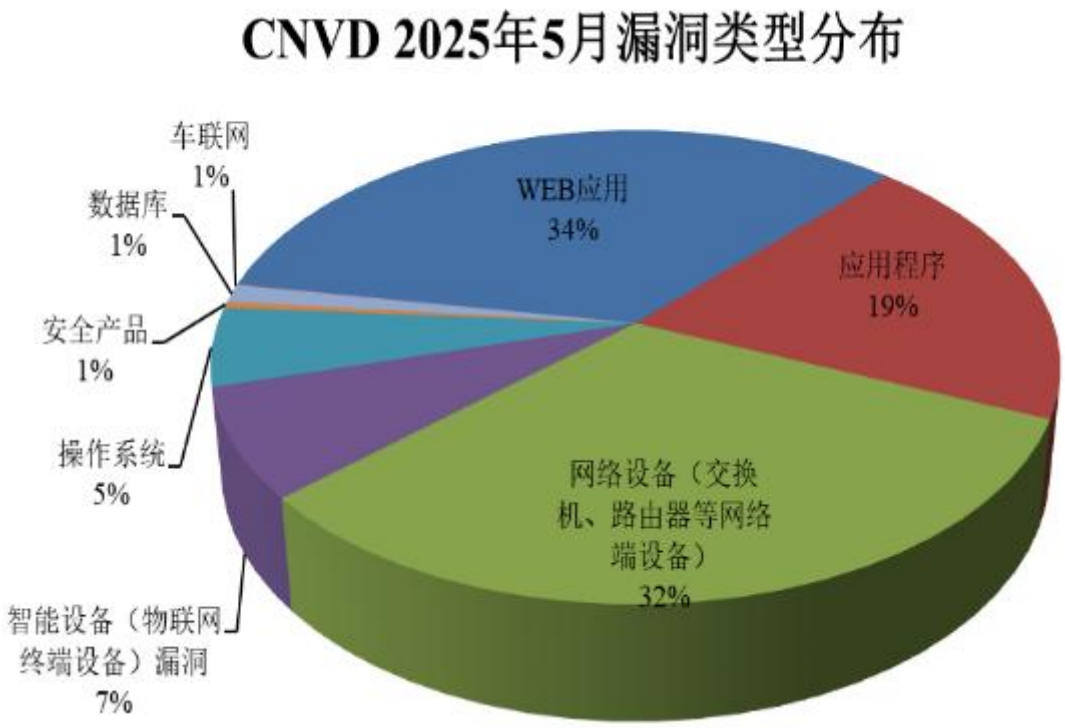
四、5 月份 CNVD 漏洞收录情况

国家信息安全漏洞共享平台（China National Vulnerability Database，以下简称 CNVD），5 月收集整理信息安全漏洞 1429 个，其中高危漏洞 753 个，中危漏洞 601 个，低危漏洞 75 个。

上述漏洞中，可被利用来实施远程网络攻击的漏洞有 1203 个，数据来源自 CNVD 站点漏洞统计数据。

（一）漏洞分类统计

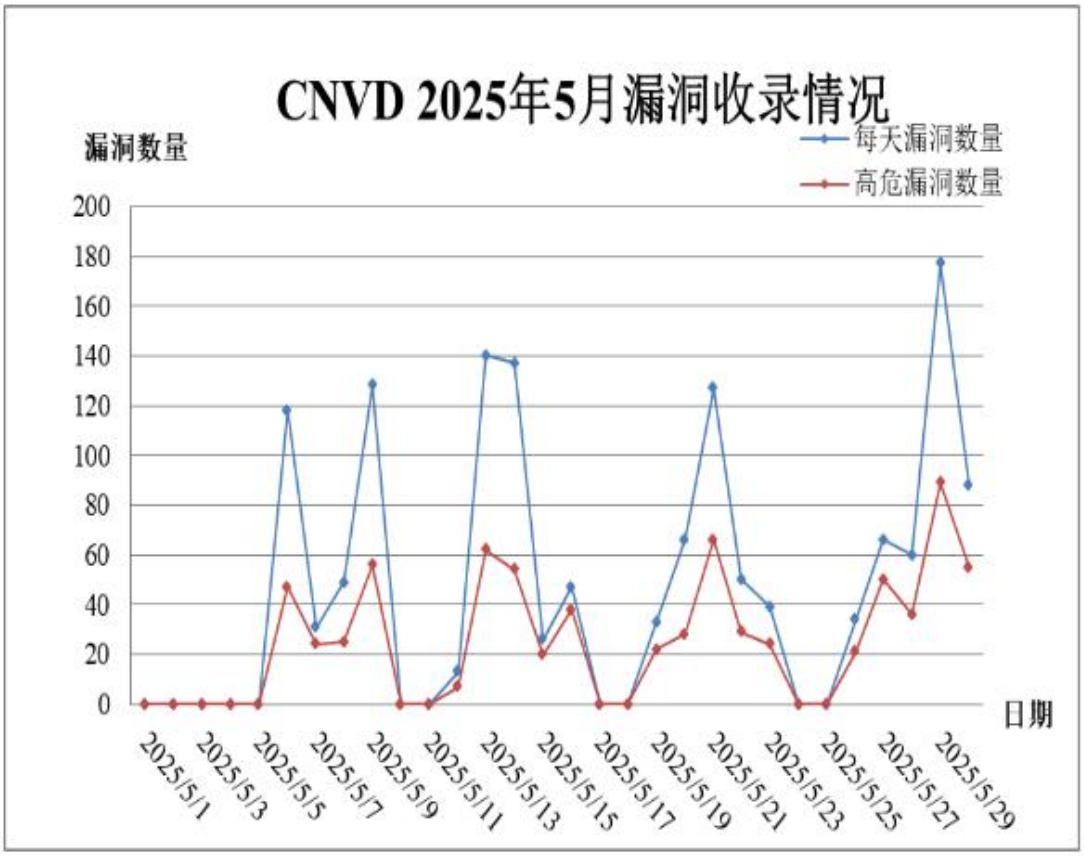
据漏洞影响对象的类型，漏洞可分为 WEB 应用、应用程序、操作系统、网络设备（交换机、路由器等网络端设备）、数据库、安全产品（如防火墙、入侵检测系统等）、智能设备（物联网终端设备）和车联网漏洞。不同类型漏洞的分布如图 1 所示，本月 WEB 应用占比例较大。与前 12 个月相比，网络设备（交换机、路由器等网络端设备）、智能设备（物联网终端设备）、操作系统、车联网漏洞的数量处于高位，应用程序、WEB 应用、数据库和安全产品漏洞的数量处于低位。



漏洞类型分布

（二）漏洞趋势

5 月，CNVD 收集整理信息安全漏洞 1429 个，与前 12 个月平均收录数量 1349 个相比，处于低位；本月高危漏洞 753 个，与前 12 个月高危漏洞平均收录数量 679 个相比，处于高位。5 月的总体漏洞趋势如图所示



5 月份漏洞发布趋势

附录：5 月份重要漏洞信息汇总

5 月份对国内用户广泛使用的信息系统和应用程序影响较大的重要漏洞如下表所示。

序号	漏洞名称	编号及影响产品信息		影响描述
1	Microsoft 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-09952、CNVD-2025-09953 CNVD-2025-09954、CNVD-2025-09955 CNVD-2025-09956、CNVD-2025-09958 CNVD-2025-10448、CNVD-2025-10449 CNVD-2025-10450、CNVD-2025-10451	本月，Microsoft 多款产品存在安全漏洞。攻击者可利用漏洞在系统上执行任意代码。本月漏洞包括：Microsoft Office 代码执行漏洞（CNVD-2025-09952、CNVD-2025-09953、CNVD-2025-09954、CNVD-2025-09955、CNVD-2025-09956、CNVD-2025-09958、CNVD-2025-10448、CNVD-2025-10449、CNVD-2025-10450、CNVD-2025-10451）等。
		其他编号	CVE-2025-24083、CVE-2025-24082 CVE-2025-24081、CVE-2025-24080 CVE-2025-24079、CVE-2025-24077 CVE-2025-29977、CVE-2025-30393 CVE-2025-30379、CVE-2025-29979	
		发布时间	2025-05-16	
		影响产	Microsoft Office 2016	

		品	Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC 2024 Microsoft Office Online Server Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC for Mac 2024 Microsoft Excel 2016	
2	Google 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-09153、CNVD-2025-09152 CNVD-2025-09151、CNVD-2025-09155 CNVD-2025-09154、CNVD-2025-09156 CNVD-2025-09157、CNVD-2025-09217 CNVD-2025-09255、CNVD-2025-10928	本月，Google 多款产品存在安全漏洞。攻击者可利用漏洞绕过操作系统验证，导致堆损坏，提交特殊 Web 请求，诱使用户解析，可提升权限等。本月漏洞包括：Google Chrome OS 越界写入漏洞（CNVD-2025-09153、CNVD-2025-09154）、Google Chrome OS 信息泄露漏洞（CNVD-2025-09152）、
		其他编号	CVE-2025-1122、CVE-2025-1566 CVE-2025-1568、CVE-2025-3620 CVE-2025-1292、CVE-2025-3619 CVE-2024-29754、CVE-2024-29741 CVE-2025-3068、CVE-2025-4372	

		发布时间	2025-05-07	Google Chrome OS 访问控制错误漏洞（CNVD-2025-09151）、Google Chrome 资源管理错误漏洞（CNVD-2025-09155）、Google Chrome 堆缓冲区溢出漏洞（CNVD-2025-09156）、Google Pixel 越界读取漏洞（CNVD-2025-09157）、Google Pixel 本地权限提升漏洞、Google Chrome 输入验证错误漏洞、Google Chrome 代码执行漏洞（CNVD-2025-10928）等。
		影响产品	Google Chrome OS Google Chrome Google Pixel	
3	IBM 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-09283、CNVD-2025-09285CNVD-2025-09286、CNVD-2025-09392CNVD-2025-10399、CNVD-2025-10398CNVD-2025-10396、CNVD-2025-10424CNVD-2025-10427、CNVD-2025-10426	本月，IBM 多款产品存在安全漏洞。攻击者可利用漏洞获取敏感信息，导致信息泄露，通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML 等。本月漏洞包括：IB
		其他编号	CVE-2025-2986、CVE-2023-42007 CVE-2023-33844、CVE-2022-438	

			51 CVE-2025-33093、CVE-2025-2898 CVE-2025-2900、CVE-2025-2950 CVE-2024-55912、CVE-2025-1838	M Maximo Asset Management 跨站脚本漏洞（CNVD-2025-09283）、IBM Sterling Control Center 跨站脚本漏洞（CNVD-2025-09285）、IBM Security Verify Governance 跨站脚本漏洞（CNVD-2025-09286）、IBM Aspera Console 加密问题漏洞、IBM Sterling Partner Engagement Manager 密钥存储不当漏洞、IBM Maximo Application Suite 权限提升漏洞、IBM Semeru Runtime 拒绝服务漏洞、IBM i 内容中和不当漏洞、IBM Concert Software 加密问题漏洞、IBM Cloud Pak for Business Automation 拒绝服务漏洞等。
		发布时间	2025-05-19	
		影响产品	IBM Maximo Asset Management IBM Maximo Application Suite IBM Security Verify Governance IBM Aspera Console IBM Sterling Control Center IBM Sterling Partner Engagement Manager IBM Semeru Runtime IBM i IBM Concert Software IBM Cloud Pak for Business Automation	

4	Adobe 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-09266、CNVD-2025-09269 CNVD-2025-09271、CNVD-2025-10390 CNVD-2025-10388、CNVD-2025-10387 CNVD-2025-10386、CNVD-2025-10393 CNVD-2025-10391、CNVD-2025-10395	本月，Adobe 多款产品存在安全漏洞。攻击者可利用漏洞通过诱使用户打开恶意文件，执行任意代码。本月漏洞包括：Adobe Bridge 缓冲区溢出漏洞、Adobe Framemaker 缓冲区溢出漏洞（CNVD-2025-09269）、Adobe Framemaker 堆缓冲区溢出（CNVD-2025-09271）、Adobe Substance3D-Stager 越界写入漏洞、Adobe Substance3D-Stager 资源管理错误漏洞（CNVD-2025-10386、CNVD-2025-10387）、Adobe ColdFusion 输入验证错误漏洞、Adobe ColdFusion 授权不当漏洞（CNVD-2025-10391、CNVD-2025-10390）、Ad
		其他编号	CVE-2025-27193、CVE-2025-30298 CVE-2025-30299、CVE-2025-43565 CVE-2025-43569、CVE-2025-43571 CVE-2025-43570、CVE-2025-43560 CVE-2025-43561、CVE-2025-43562	
		发布时间	2025-05-19	
		影响产品	Adobe Bridge Adobe Framemakers Adobe ColdFusion Adobe Substance3D - Stager	

				obe ColdFusion 命令注入漏洞等。
5	Tenda 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-10819、CNVD-2025-10821 CNVD-2025-10824、CNVD-2025-10823 CNVD-2025-10825、CNVD-2025-10827 CNVD-2025-10826、CNVD-2025-11167 CNVD-2025-11166、CNVD-2025-11212	本月，Tenda 多款产品存在安全漏洞。攻击者可利用漏洞导致拒绝服务。本月漏洞包括：Tenda FH1201 缓冲区溢出漏洞（CNVD-2025-10819、CNVD-2025-10821、CNVD-2025-10824、CNVD-2025-10823、CNVD-2025-10825、CNVD-2025-10827、CNVD-2025-10826、CNVD-2025-11167、CNVD-2025-11166、CNVD-2025-11212）等。
		其他编号	CVE-2024-42943、CVE-2024-42942 CVE-2024-42940、CVE-2024-42941 CVE-2024-42944、CVE-2024-42946 CVE-2024-42945、CVE-2024-42951 CVE-2024-42950、CVE-2024-42952	
		发布时间	2025-05-26	
		影响产品	Tenda FH1201	

6	TOTOLINK 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-09853、CNVD-2025-09852 CNVD-2025-09856、CNVD-2025-09855 CNVD-2025-09854、CNVD-2025-09857 CNVD-2025-09867、CNVD-2025-09871 CNVD-2025-09933、CNVD-2025-09944	本月，TOTOLINK 多款产品存在安全漏洞。攻击者可利用漏洞控制目标计算机或破解其数据，导致命令注入，在系统上执行任意代码或者导致拒绝服务等。本月漏洞包括：TOTOLINK N150RT /boafrm/formStaticDHCP 文件缓冲区溢出漏洞、TOTOLINK N150RT /boafrm/formPortFw 文件缓冲区溢出漏洞、TOTOLINK N150RT /boafrm/formWlwds 文件缓冲区溢出漏洞、TOTOLINK N150RT /boafrm/formWdsEncrypt 文件缓冲区溢出漏洞、TOTOLINK N150RT /boafrm/formVlan 文件缓冲区溢出漏洞、TOTOLINK N150RT 缓冲
		其他编号	CVE-2025-3989、CVE-2025-3988 CVE-2025-3992、CVE-2025-3991 CVE-2025-3990、CVE-2025-3993 CVE-2024-8573、CVE-2024-8575 CVE-2025-28017、CVE-2025-3987	
		发布时间	2025-05-15	
		影响产品	TOTOLINK N150RT TOTOLINK AC1200 T8 TOTOLINK AC1200 T10 TOTOLINK A800R	

				区溢出漏洞、TOTOLINK AC1200 T8 和 AC1200 T10 cstecgi.cgi 文件 setParentalRules 函数缓冲区溢出漏洞、TOTOLINK AC1200 缓冲区溢出漏洞、TOTOLINK A800R 命令注入漏洞（CNVD-2025-09933）、TOTOLINK N150RT 命令注入漏洞（CNVD-2025-09944）等。
7	Dell 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-09170、CNVD-2025-09394 CNVD-2025-09398、CNVD-2025-09397 CNVD-2025-09396、CNVD-2025-09399 CNVD-2025-09680、CNVD-2025-09679 CNVD-2025-09683、CNVD-2025-09684	本月，Dell 多款产品存在安全漏洞。攻击者可利用漏洞修改配置，获得对未经授权数据的访问权限，导致拒绝服务等。本月漏洞包括：Dell PowerScale OneFS 拒绝服务漏洞、Dell PowerProtect Data Manager Reporting 权限提升漏洞、Dell Trusted Dev
		其他编号	CVE-2022-34371、CVE-2025-23375 CVE-2025-29984、CVE-2025-29983	

			CVE-2025-21105、CVE-2025-27690 CVE-2025-26480、CVE-2025-22471 CVE-2025-29982、CVE-2025-27693	ice 权限提升漏洞、Dell Trusted Device 后置链接漏洞、Dell RecoverPoint for Virtual Machines 命令执行漏洞、Dell PowerScale OneFS 默认密码漏洞、Dell PowerScale OneFS 资源消耗漏洞、Dell PowerScale OneFS 整数溢出漏洞、Dell Wyse Management Suite WMS 授权问题漏洞、Dell Wyse Management Suite 跨站脚本漏洞等。
		发布时间	2025-05-12	
		影响产品	DELL PowerScale OneFS|9.3.0.6 DELL PowerProtect Data Manager Reporting Dell Trusted Device Dell RecoverPoint for Virtual Machines Dell PowerScale OneFS DELL Dell Wyse Management Suite WMS DELL Dell Wyse Management Suite	
8	**NETGEAR 多款产品存在安全漏洞**	**CNVD 编号**	CNVD-2025-09918、CNVD-2025-09917 CNVD-2025-09916、CNVD-2025-09922 CNVD-2025-09920、CNVD-2025-09919 CNVD-2025-10402、CNVD-2025-10400	本月，NETGEAR 多款产品存在安全漏洞。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。本月漏洞包括：NETGEAR EX6200 sub_3C03C

			CNVD-2025-10417、CNVD-2025-10416	函数缓冲区溢出漏洞、NETGEAR EX6120 sub_30394 函数缓冲区溢出漏洞、NETGEAR EX6120 fwAcosCgiInbound 函数缓冲区溢出漏洞、NETGEAR JWNR2000v2 default_version_is_new 函数缓冲区溢出漏洞、NETGEAR JWNR2000v2 check_language_file 函数缓冲区溢出漏洞、NETGEAR EX6200 sub_3C8EC 函数缓冲区溢出漏洞、NETGEAR JWNR2000v2 sub_4238E8 函数缓冲区溢出漏洞、NETGEAR JWNR2000v2 get_cur_lang_ver 函数缓冲区溢出漏洞、NETGEAR EX6200 sub_47F7C 函数缓冲区溢出漏洞、NETGEAR EX6200 sub_4
		其他编号	CVE-2025-4141、CVE-2025-4140 CVE-2025-4139、CVE-2025-4115 CVE-2025-4114、CVE-2025-4142 CVE-2025-4120、CVE-2025-4116 CVE-2025-4147、CVE-2025-4146	
		影响产品	2025-05-16	
		CNVD 编号	NETGEAR EX6200 NETGEAR EX6120 NETGEAR JWNR2000v2	

				1940 函数缓冲区溢出漏洞等。