深信服智安全
SANGFOR SECURITY

# 网络安全半月刊

（20250421 期）

深信服科技股份有限公司

2025 年 4 月 21 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 4 月份(4.1-4.21)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 Vite 任意文件读取漏洞，CNVD 和微软发布了安全通告及漏洞详情，建议受影响用户及时更新升级至最新版本。

**本期网络安全政策法律动态信息：**

**国内政策法规：**

1、《2025 年工业和信息化标准工作要点》印发

2、网安标委下达 14 项网络安全推荐性国家标准计划

3、6 项网络安全国家标准获批发布

**国际政策法规：**

1、欧盟委员会发布《保护欧盟》战略，旨在提升内部安全与抵御混合威胁能力

2、马来西亚组建网络战部队

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、《2025 年工业和信息化标准工作要点》印发

4 月 8 日，工业和信息化部办公厅发布关于印发 2025 年工业和信息化标准工作要点的通知。提出今年将围绕健全构建现代化产业体系，实施《新产业标准化领航工程实施方案（2023—2035 年）》，持续完善新兴产业标准体系建设，前瞻布局未来产业标准研究，制定行业标准 1800 项以上，组建 5 个以上新兴产业和未来产业标准化技术组织。围绕筑牢产业发展安全底线，编制工业和信息化强制性国家标准体系建设指南，组织编制强制性国家标准 100 项以上。围绕推动产业全球化发展，支持 100 项以上由我国企事业单位牵头制定的国际标准，全行业国际标准转化率达到 88%。提升行业治理能力现代化水平，为推进新型工业化，加快建设制造强国和网络强国提供坚强保障。
原文链接：
https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2025/art_02f418da5c244531b408b1eac63f1cf8.html

### 2、网安标委下达 14 项网络安全推荐性国家标准计划

4 月 9 日，网安标委正式下达 14 项网络安全推荐性国家标准制定计划，重点覆盖数据安全、关键信息基础设施保护、人工智能安全等热点领域。新计划包括《信息安全技术 政务云服务安全能力要求》《信息安全技术 智能网联汽车数据安全指南》等标准，旨在细化《网络安全法》《数据安全法》的落地规范，为数字政府、智慧交通等场景提供技术支撑。标准由中国电子技术标准化研究院、国家信息技术安全研究中心等机构牵头编制，拟于 2026 年底前完成。网安标委指出，此次标准将聚焦数据跨境流动、AI 伦理风险等新兴挑战，推动企业完善安全防护体系。尽管为推荐性标准，但其内容与行业监管趋势深度契合，企业积极采纳可提升合规竞争力。

原文链接：
https://baijiahao.baidu.com/s?id=1828972967226751014&wfr=spider&for=pc
https://baijiahao.baidu.com/s?id=1828972967226751014&wfr=spider&for=pc

### 3、6 项网络安全国家标准获批发布

中国信息安全公众号 4 月 9 日发文，根据 2025 年 3 月 28 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2025 年第 6 号），全国网络安全标准化技术委员会归口的 6 项国家标准正式发布。具体清单如下：

| 序号 | 标准编号 | 标准名称 | 实施日期 |
|---|---|---|---|
| 1 | GB/T 45409-2025 | 网络安全技术 运维安全管理产品技术规范 | 2025/10/1 |
| 2 | GB/T 45389-2025 | 数据安全技术 数据安全评估机构能力要求 | 2025/10/1 |
| 3 | GB/T 45392-2025 | 数据安全技术 基于个人信息的自动化决策安全要求 | 2025/10/1 |
| 4 | GB/T 45396-2025 | 数据安全技术 政务数据处理安全要求 | 2025/10/1 |
| 5 | GB/T 45404-2025 | 数据安全技术 大型互联网企业内设个人信息保护监督机构要求 | 2025/10/1 |
| 6 | GB/T 45406-2025 | 网络关键设备安全技术要求 可编程逻辑控制器（PLC） | 2025/10/1 |

原文链接：
https://mp.weixin.qq.com/s/w3itdO4bjaEwHbVCsQkk3g
https://mp.weixin.qq.com/s/w3itdO4bjaEwHbVCsQkk3g

## （二）国际政策法规：

### 1、欧盟委员会发布《保护欧盟》战略，旨在提升内部安全与抵御混合威胁能力

近日，欧盟委员会发布《保护欧盟》战略，旨在协助成员国提高确保公民安全的能力，增强对混合威胁的抵御能力。该战略通过建立更强大的法律框架、加强信息共享和合作，保护关键基础设施、加强网络安全和打击网络威胁。该战略

指出，对关键基础设施的威胁是一个主要问题，特别是连接成员国的基础设施。在网络安全方面，委员会将更广泛地关注信息通信技术供应链和基础设施的安全性和弹性，改进欧洲网络安全认证框架，并鼓励关键实体选择提供适当网络安全水平的云和电信服务。

原文链接：
https://mp.weixin.qq.com/s/6JH8u6uxWBTQ56AnkcpFZQ

### 2、马来西亚组建网络战部队

据报道，马来西亚国防部近期宣布，将组建一支专业化网络战部队。该部队主要负责网络威胁情报分析、网络恐怖袭击应急响应、网络攻击取证溯源，以及保障国防和关键军民设施的网络安全。有评论认为，这是马来西亚武装力量推进数字防务转型、增强多域作战能力的关键举措。随着新加坡、菲律宾和印度尼西亚等国纷纷公布军力转型计划，东南亚地区在网络空间的军备竞赛正日益加剧。

原文链接：
https://mp.weixin.qq.com/s/9FYx2LeEeTrYkItb9f1apw

## 二、安全热点时事资讯

### （一）国内安全事件

### 1、郝某出卖国家秘密，因间谍罪被判处无期徒刑

**时间：**4 月 11 日

**概况：**据央视新闻报道，近期，国家安全机关破获一起重大间谍案件。经查，犯罪嫌疑人郝某受境外间谍情报机关指挥，长期潜伏在我核心要害部门窃取情报，最终因间谍罪被判处无期徒刑。经鉴定，郝某向境外间谍情报机关提供的情报，涉及中央某部敏感项目及内部人员情况，其中机密级国家秘密 5 项、秘密级国家秘密 2 项，刑法第一百一十一条规定的情报 14 项。

**警示：**基于此事件，国家安全机关给出如下警示：境外间谍情报机关长期觊觎我留学人员群体，并利用签证环节物色有价值的目标对象，主动进行贴靠。以签证

官身份出现的情报人员，对于涉世未深的年轻学生而言，具有很强的欺骗性。国家安全机关掌握，请客吃饭、邀请旅游、赠送礼品、提供兼职等都是境外间谍情报机关人员拉拢我留学人员的常用手段。待关系密切、时机成熟就会实施策反。境外间谍情报机关及其代理人始终紧盯我核心要害部门，大肆对我重点领域开展情报渗透窃密活动，严重威胁我国家安全和发展利益。

原文链接：

https://mp.weixin.qq.com/s/wC2kkthVDyB57bDU9txadw

**2、湖北公安网安部门查处一起利用 AI 工具编造虚假信息案**

**时间：**4 月 20 日

**概况：**公安网安局发文，发现某资讯网站发布的文章严重失实。公安机关根据相关法律法规，对涉事公司予以行政处罚。目前，涉事公司已在网站首页公开致歉声明，下架全部 AI 生成内容，并在公司内进行整改。

据查，该公司为提高所运营网站的流量，购买了一个 AI 智能写作软件，通过输入自设的关键词，由系统自动抓取网络信息生成文章。涉案文章系 AI 机械拼接多地文本而成，该公司发布前未按规定对发布内容履行审核责任。

**警示：**

根据《互联网信息服务深度合成管理规定》，任何组织和个人不得利用深度合成服务制作、复制、发布、传播 法律、行政法规禁止的信息，不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动。

深度合成服务提供者和使用者不得利用深度合成服务制作、复制、发布、传播虚假新闻信息，转载基于深度合成服务制作发布新闻信息的，应当依法转载互联网信息稿源单位发布的新闻信息。

深度合成服务提供者和技术支持者违反《互联网信息服务深度合成管理规定》的，依照有关法律、行政法规的规定处罚；造成严重后果的，依法从重处罚。构成违反治安管理行为的，由公安机关依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

原文链接：

https://mp.weixin.qq.com/s/tpCAv_tDWccM2YcsXMafsA

### 3、某机关工作人员违规使用扫描软件导致重大泄密

**时间：**4 月 20 日

**概况：**据国家安全部发文，近期某机关工作人员因贪图便利，违规使用互联网扫描软件扫描涉密会议纪要，使该文件被自动备份至网盘。但其网盘账号密码遭暴力破解，使得攻击者获取了其在 3 年间扫描的 127 份涉密文件，后泄露文件经境外社交媒体传播，造成重大失泄密事件，对我国家安全构成现实威胁。

**警示：**

国家安全无小事，保密没有“局外人”，广大人民群众，特别是涉密岗位工作人员，要切实提高安全意识，自觉规范软件应用使用行为，做好信息安全防护。

对于企业来说，也要加强涉密信息保护。严禁通过任何互联网渠道传输、保存或处理涉密资料。严禁使用联网扫描软件扫描识别涉密信息，不能以方便工作为由将涉密文件在线上储存。谨慎选择扫描软件。尽量从官方应用商店下载经过安全认证的扫描软件，以降低下载到恶意软件的风险。严格管控软件权限。在安装扫描软件时，仔细查看软件申请的权限列表。只授予软件运行所必需的权限，加强数据存储安全。慎重选择服务商提供的照片、通讯录等信息自动备份到云端功能。在将数据进行云端存储之前，可通过专业软件对数据进行加密，或者使用云盘自带的加密功能，

原文链接：

https://mp.weixin.qq.com/s/aXGEuecSzj4EUCeFYvK-Wg

## （二）国际安全事件

**1、多家大型养老基金超 2 万个账号遭入侵，至少数百万元养老储蓄金被盗**

**时间：**4 月 5 日

**概况：**据路透社 4 月 5 日报道，黑客在一系列协调攻击中针对澳大利亚主要养老金基金展开行动，盗取了部分会员的储蓄，并泄露了超过 20000 个账户的信息。

澳大利亚国家网络安全协调员米歇尔·麦金尼斯在声明中表示，她已经得知“网络犯罪分子”正在攻击该国 4.2 万亿澳元（IT 之家注：现汇率约合 18.71 万亿元人民币）退休储蓄领域的账户，政府正与监管机构及行业合作，组织应对措施。该国总理安东尼·阿尔巴内塞表示，他已接到黑客攻击的报告，政府将作出“深思熟虑”的回应。他补充道，类似攻击在澳大利亚频繁发生，平均每六分钟就有一起。

**安全防御建议：（适配金融、基础设施行业的大型企业和单位机构）**

1.强化用户认证与访问控制：采用多因素认证方式，如密码、指纹、短信验证码等相结合，增加账号登录的安全性，降低被破解的概率。严格控制员工对账户信息的访问权限，根据岗位职责和业务需求进行精准授权，避免过度授权。

2.加强系统维护与漏洞管理：定期对信息系统进行全面检查和评估，及时安装操作系统、数据库、应用程序等的安全补丁，修复可能被黑客利用的漏洞。

3.建立实时监控与预警机制：部署专业的网络安全监控设备和软件，实时监测网络流量、异常登录行为、数据传输等情况，一旦发现可疑活动，立即发出警报并采取相应措施。

4.开展员工安全培训与教育：定期组织员工参加网络安全培训，让员工了解常见的网络攻击手段和防范方法，如钓鱼邮件、社交工程等，提高员工的安全意识和警惕性。

5.完善应急响应计划：制定详细的应急响应预案，明确在遭遇账号入侵、数据泄露等事件时的应对流程和责任分工，定期进行应急演练，确保在事件发生时能够迅速、有效地进行处置，最大程度减少损失。

原文链接：

https://baijiahao.baidu.com/s?id=1828526075633003701&wfr=spider&for=p

c

**2、知名工业制造上市公司森萨塔遭勒索攻击，生产运营被迫中断**

**时间：**4 月 6 日

**概况：**美国上市公司森萨塔科技（Sensata Technologies）上周末遭遇勒索软件攻击，公司网络内的部分设备遭到加密，致使业务运营中断。

此次攻击发生于 4 月 6 日（星期日），并涉及数据被窃取的情况。此次事件已对森萨塔的运营造成暂时影响，包括发货、收货、制造生产以及其他多个支持职能。在外部网络安全专家的协助下，初步调查确认黑客已从公司网络中窃取了数据。森萨塔表示，公司已立即采取措施，加快受此次网络攻击影响的关键功能的恢复工作。

**安全防御建议：（适配企业尤其是工业制造业企业）**

1.加强网络安全防护体系建设：进行全面的安全评估，加强防火墙、入侵检测系统、防病毒软件等安全设备的部署和配置，形成多层次的安全防护体系。尤其要重视 IT 与 OT 网络的隔离，防止攻击者通过 VPN 漏洞、远程桌面协议等薄弱点入侵。

2.建立可靠的备份与恢复系统：采用多重保障的系统备份策略，包括将备份数据与主网络物理隔离，防止加密蔓延；保留多时间点备份版本，应对潜伏期攻击；通过自动化工具检测备份异常访问模式，保证备份的有效性。定期对备份数据进行恢复演练，确保在遭受攻击时能够快速恢复关键业务数据和系统。

3.强化供应链安全管理：对第三方供应商进行严格的安全评估和管理，要求供应商遵守企业的网络安全标准，确保其提供的产品和服务不存在安全漏洞。

4.提高安全意识与应急能力：组织员工参加工业网络安全培训，提高员工对勒索软件等网络威胁的认识和防范能力。定期开展应急演练，模拟勒索软件攻击等场景，检验和提升企业的应急响应能力。

原文链接：

http://www.cnetsec.com/dfaq_wordpress/?p=42467

### 3、俄罗斯 APT 组织利用设备码钓鱼技术绕过多因素认证，具有全球性影响

**时间：**4 月 13 日

**概况：**俄罗斯国家支持的 APT 组织 Storm-2372 近期发起了一场复杂的网络攻击活动，利用设备码钓鱼（Device Code Phishing）技术绕过多因素认证（MFA）安全措施。这种针对性攻击手段标志着威胁行为者通过社会工程学突破高级安全系统的能力显著提升，攻击者可以在不触发传统安全警报的情况下，未经授权访问高价值目标。

该攻击活动主要针对政府机构、科技公司、金融机构、国防承包商、医疗机构和媒体组织等多个领域内拥有重要数据和战略影响力的机构。研究人员已在美国、乌克兰、英国、德国、加拿大和澳大利亚等多个国家发现了这些攻击的数字证据，表明该行动具有全球性影响。

**安全防御建议：（适配所有企业）**

为防范这些复杂攻击，网络安全专业人员应采取以下措施：

实施基于设备合规性和地理位置限制认证的条件访问策略；定期审核 OAuth 令牌请求；部署使用 FIDO2 安全密钥而非基于短信验证的防钓鱼 MFA 解决方案；开展全面的安全意识培训，特别关注这些新兴威胁。

原文链接：

https://mp.weixin.qq.com/s/xNPkCp3MbOU2o1XgIVuTpA

### 4、4chan 遭黑客攻击下线，管理员信息及源代码疑遭泄露

**时间：**4 月 14 日

**概况：**当地时间 4 月 14 日，运营超二十年的老牌匿名论坛 4chan 遭遇了一次严重的网络安全事件。该网站在当天早些时候突然无法访问，随后长时间处于下线状态。4chan 论坛于 2003 年创建，是互联网上最早、最臭名昭著也最具影响力的匿名讨论版之一，多次成为黑客或内部人士泄露敏感信息的场所，涉及的公司包括微软、英特尔、Valve、Twitch 及迪士尼等。有黑客组织声称对此负责，并表示已获取该网站管理员的敏感信息及网站源代码。事件发生后，一个名为 Soyjak.party 的网络社群(亦被称为 TheParty)成员公开宣称发动了此次攻击。

该组织成员在网络上发布信息称，一名黑客已渗透 4chan 系统长达一年，并于 4 月 14 日执行了攻击行动。截至目前，4chan 官方尚未就此次攻击事件发布正式声明。

**安全防御建议：（适配所有企业）**

此次安全事件暴露出的潜在数据泄露风险和平台陈旧的技术架构问题，已引发网络安全领域的关注。企业需加强对官方网站的安全性管理，对网站技术架构进行全面评估和升级，淘汰陈旧的硬件设备和软件系统，采用先进的安全技术和框架，如微隔离、零信任架构等，提高系统的安全性和稳定性。加强服务器的安全防护，配置防火墙、入侵防御系统等安全设备，防止黑客的非法入侵。同时加强代码安全管理：建立严格的代码审查制度，对网站的源代码进行定期审查和安全检测，及时发现和修复潜在的安全漏洞。

原文链接：

https://mp.weixin.qq.com/s/7NMeBGzH59Er2nMNocYibw

**5、英国软件公司 Logezy 由于员工管理数据库配置错误，泄露 800 万英国医疗保健工作者信息**

**时间：**4 月 16 日

**概况：**vpnMentor 的网络安全研究员兼 Security Discovery 联合创始人 Jeremiah Fowler 最近发现了一起重大数据泄露事件，涉及一家专门从事员工数据管理的英国软件公司 Logezy。根据 Fowler 分享的调查结果，泄露的数据揭示了近 800 万条记录，总计 1.1TB 的数据（7975438 个文件），存储在缺乏密码保护和加密的数据库中。暴露的数据库包含敏感信息，包括工作授权文件、国民保险号码、证书、电子签名、时间表、用户图像和政府颁发的身份证件。

这种数据泄露带来了巨大的风险，尤其是在医疗保健行业，该行业越来越成为网络攻击的目标。泄露的信息可能被用于恶意目的，包括身份盗窃。犯罪分子可能会利用窃取的数据冒充医护人员的身份，以获取经济利益。

**安全防御建议：（适配数据安全管理强相关企业）**

1. 强化数据访问控制：严格设定员工对数据的访问权限，遵循“最小权限原则”，

仅授予员工为完成工作所必需的数据访问级别。对于敏感数据实行更严格的访问审批流程，避免数据被过度访问或滥用。

2. 加密敏感数据：对存储在数据库中的敏感信息采用强加密算法进行加密处理。确保即使数据被非法获取，攻击者也无法轻易解密和使用这些信息。在数据传输过程中，同样使用加密技术，防止数据在传输过程中被截获和窃取。

3.严格数据库安全管理：对数据库进行定期的安全评估和漏洞扫描，及时发现并修复潜在的安全漏洞。确保数据库的密码设置强度足够，采用复杂的密码组合，并定期更换密码。同时，开启数据库的审计功能，记录对数据库的所有访问操作，以便在发生安全事件时能够进行追溯和调查。

4.提升网络安全防护能力：部署先进的网络安全设备，实时监测网络流量，防止外部攻击者入侵企业网络。对企业内部网络进行分段管理，限制不同区域之间的数据流动，降低数据泄露的风险。

5.员工安全培训与教育：定期组织员工参加网络安全培训，提高员工对数据安全的认识和重视程度。培训内容应包括如何识别和防范网络钓鱼攻击、如何保护敏感数据、以及数据泄露的严重后果等。

原文链接：https://www.zzwa.org.cn/8957/

## （三）国际安全热点

### 1、全球通用漏洞数据库项目(CVE)面临资金危机

4 月 15 日，美国非营利研发组织 MITRE 宣布，其与美国国土安全部（DHS）签订的"通用漏洞披露（CVE）"数据库维护合同将于 2025 年 4 月 16 日午夜到期。这个运行 25 年的项目作为网络安全防御体系的核心支柱，因美国国土安全部未说明具体原因拒绝续约而面临终止。媒体广泛报道后，在合同即将到期的最后时刻，2025 年 4 月 16 日星期三上午，美国国土安全部下属单位网络安全和基础设施安全局（CISA） 与 MITRE 签署了一份 11 个月的合同延期，未来会怎

么很难说，毕竟 CISA 已经历两次资金削减，40%的员工（约 1300 名）被解雇。然而，这一事件暴露了 CVE 项目对美国政府资助的高度依赖性。为确保项目的可持续性和中立性，部分 CVE 董事会成员提出成立独立的非营利组织“CVE 基金会”，以推动项目向社区驱动模式转型。

原文链接：

https://mp.weixin.qq.com/s/G1rIAQel13z_GnmED9opAQ

https://mp.weixin.qq.com/s/BhkAb6OOHL3Yeg3QKZ26Hw

## 2、谷歌发布网络安全 AI 新模型 Sec-Gemini v1 并免费开放

谷歌近日宣布推出实验性 AI 模型 Sec-Gemini v1，旨在通过人工智能技术革新网络安全防御体系。该模型由 Sec-Gemini 团队成员 Elie Burzstein 和 Marianna Tishchenko 共同研发，旨在帮助网络安全人员应对日益复杂的网络威胁。

谷歌表示，推进 AI 驱动的网络安全需要行业协同努力。为促进合作，Sec-Gemini v1 将免费向选定的组织、机构、专业人士和非政府组织开放用于研究目的。有意者可通过谷歌提供的表格申请早期访问权限。随着网络威胁不断演变，此类工具有望帮助防御方在与攻击者的对抗中占据更有利位置。

原文链接：

https://mp.weixin.qq.com/s/nby9RF_j9zCkWkigDTOFEw

# 三、安全风险通告

## （一） Vite 任意文件读取漏洞(CVE-2025-31125)

**漏洞名称** ：Vite 任意文件读取漏洞(CVE-2025-31125)

**漏洞描述**：2025 年 4 月 1 日，深瞳漏洞实验室监测到一则 Vite 组件存在任意文件读取漏洞的信息。Vite 存在一个任意文件读取漏洞，未授权的**攻击者可以构造恶意的 HTTP 请求读取任意文件，导致敏感信息泄露**。

漏洞编号：CVE-2025-31125，漏洞威胁等级：**中危**。

**组件介绍：**

Vite 是一个现代化的前端构建工具，它利用了浏览器原生 ES 模块导入的能力来提供快速的开发服务器和构建性能。Vite 旨在优化开发体验，通过即时模块热更新（HMR）等技术，使得开发过程更加高效。

**影响范围：**

目前受影响的 Vite 版本：

Vite ≤ 4.5.10

5.0.0 ≤ Vite ≤ 5.4.15

6.0.0 ≤ Vite ≤ 6.0.12

6.1.0 ≤ Vite ≤ 6.1.2

6.2.0 ≤ Vite ≤ 6.2.3

**利用条件：**

1、用户认证：不需要用户认证

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，无需授权可导致敏感信息泄露。

<综合评定威胁等级>：中危，能导致敏感信息泄露。

**官方解决方案：**

官方已修复该漏洞，建议受影响用户将服务器更新到以下版本：

Vite 6.2.4

Vite 6.1.3

Vite 6.0.13

Vite 5.4.16

Vite 4.5.11

**链接如下：**

https://github.com/vitejs/vite/releases

**深信服解决方案：**

**1、风险资产发现**

支持对 Vite 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:0032127。

**【深信服漏洞评估工具 TSS】**已发布资产检测方案，指纹 ID:0032127

**2、漏洞主动检测**

支持对 Vite 任意文件读取漏洞(CVE-2025-31125)的主动检测，可批量快速检出业务场景中是否存在漏洞风险，相关产品如下：

**【深信服云镜 YJ】**已发布检测方案，规则 ID:SF-2025-00365。

**【深信服漏洞评估工具 TSS】**已发布检测方案，规则 ID:SF-2025-00994。

**【深信服安全托管服务 MSS】**已发布检测方案（需要具备 TSS 组件能力），规则 ID:SF-2025-00994。

**【深信服安全检测与响应平台 XDR】**已发布检测方案（需要具备云镜组件能力），规则 ID:SF-2025-00365。

**3、漏洞安全监测**

支持对 Vite 任意文件读取漏洞(CVE-2025-31125)的监测，可依据流量收集实时监控业务场景中的**受影响资产情况，快速检查受影响范围**，相关产品及服务如下：

**【深信服安全感知管理平台 SIP】**已发布监测方案，规则 ID:11027472。

**【深信服安全托管服务 MSS】**已发布监测方案（需要具备 SIP 组件能力），规则 ID:11027472。

**【深信服安全检测与响应平台 XDR】**已发布监测方案，规则 ID:11027472。

**4、漏洞安全防护**

支持对 Vite 任意文件读取漏洞(CVE-2025-31125)的防御，**可阻断攻击者针对该事件的入侵行为**，相关产品及服务如下：

**【深信服下一代防火墙 AF】**已发布防护方案，规则 ID:11027472。

**【深信服 Web 应用防火墙 WAF】**已发布防护方案，规则 ID:11027472。

**【深信服安全托管服务 MSS】**已发布防护方案（需要具备 AF 组件能力），规则 ID:11027472。

**【深信服安全检测与响应平台 XDR】**已发布防护方案（需要具备 AF 组件能力），规则 ID:11027472。

## （二） Vite 任意文件读取漏洞(CVE-2025-31486)

**漏洞名称** ：Vite 任意文件读取漏洞(CVE-2025-31486)

**漏洞描述**：2025 年 4 月 8 日，深瞳漏洞实验室监测到一则 Vite 组件存在任意文件读取漏洞的信息。Vite 存在一个任意文件读取漏洞，允许未授权**攻击者使用.svg 或相对路径绕过 server.fs.deny，导致敏感数据泄露**。

漏洞编号：CVE-2025-31486，漏洞威胁等级：**中危**。

**组件介绍：**

Vite 是一个现代化的前端构建工具，它利用了浏览器原生 ES 模块导入的能力来提供快速的开发服务器和构建性能。Vite 旨在优化开发体验，通过即时模块热更新（HMR）等技术，使得开发过程更加高效。

**影响范围：**

目前受影响的 Vite 版本：

Vite ≤ 4.5.11

5.0.0 ≤ Vite ≤ 5.4.16

6.0.0 ≤ Vite ≤ 6.0.13

6.1.0 ≤ Vite ≤ 6.1.3

6.2.0 ≤ Vite ≤ 6.2.4

**利用条件：**

1、用户认证：不需要用户认证

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，可造成远程代码泄露。

<综合评定威胁等级>：中危，能造成敏感信息泄露。

**官方解决方案：**

官方已修复该漏洞，建议受影响用户将服务器更新到以下版本：

Vite 6.2.5

Vite 6.1.4

Vite 6.0.14

Vite 5.4.17

Vite 4.5.12

**链接如下：**

https://github.com/vitejs/vite/releases

**深信服解决方案：**

**1、风险资产发现**

支持对 Vite 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:0032127。

**【深信服漏洞评估工具 TSS】**已发布资产检测方案，指纹 ID:0032127。

**2、漏洞主动检测**

支持对 Vite 任意文件读取漏洞(CVE-2025-31486)的主动检测，可批量快速检出业务场景中是否存在**漏洞风险**，相关产品如下：

**【深信服云镜 YJ】**已发布检测方案，规则 ID:SF-2025-00366。

**【深信服漏洞评估工具 TSS】**已发布检测方案，规则 ID:SF-2025-00992。

**【深信服安全托管服务 MSS】**已发布检测方案（需要具备 TSS 组件能力），规则 ID:SF-2025-00992。

**【深信服安全检测与响应平台 XDR】**已发布检测方案(需要具备云镜组件能力)，规则 ID:SF-2025-00366。

**3、漏洞安全监测**

支持对 Vite 任意文件读取漏洞(CVE-2025-31486)的监测，可依据流量收集实时监控业务场景中的**受影响资产情况，快速检查受影响范围**，相关产品及服务如下：

**【深信服安全感知管理平台 SIP】**已发布监测方案，规则 ID:11027474。

**【深信服安全托管服务 MSS】**已发布监测方案（需要具备 SIP 组件能力），规则 ID:11027474。

**【深信服安全检测与响应平台 XDR】**已发布监测方案，规则 ID:11027474。

**4、漏洞安全防护**

支持对 Vite 任意文件读取漏洞(CVE-2025-31486)的防御，可阻断攻击者针对该事件的入侵行为，相关产品及服务如下：

**【深信服下一代防火墙 AF】**已发布防护方案，规则 ID:11027474。

**【深信服 Web 应用防火墙 WAF】**已发布防护方案，规则 ID:11027474。

**【深信服安全托管服务 MSS】**已发布防护方案（需要具备 AF 组件能力），规则 ID:11027474。

**【深信服安全检测与响应平台 XDR】**已发布防护方案（需要具备 AF 组件能力），规则 ID:11027474。

## 四、微软安全通告

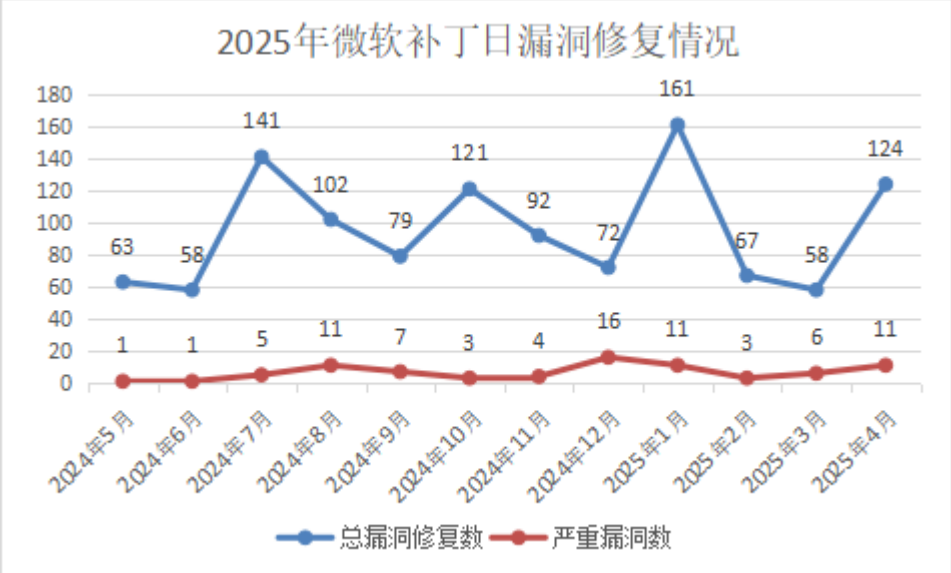
### （一） 漏洞概要

2025 年 4 月 9 日（北京时间），微软发布了 2025 年 4 月安全更新，共发布了 124 个 CVE 的补丁程序，同比上月增加了 66 个。

在漏洞安全等级方面，存在 11 个标记等级为“Critical”的漏洞，111 个漏洞被标记为“Important/High”等级的漏洞；在漏洞类型方面，主要有 33 个远程代码执行漏洞，49 个权限提升漏洞以及 16 个信息泄露漏洞。

### （二） 漏洞数据分析

#### 1、 漏洞数量趋势

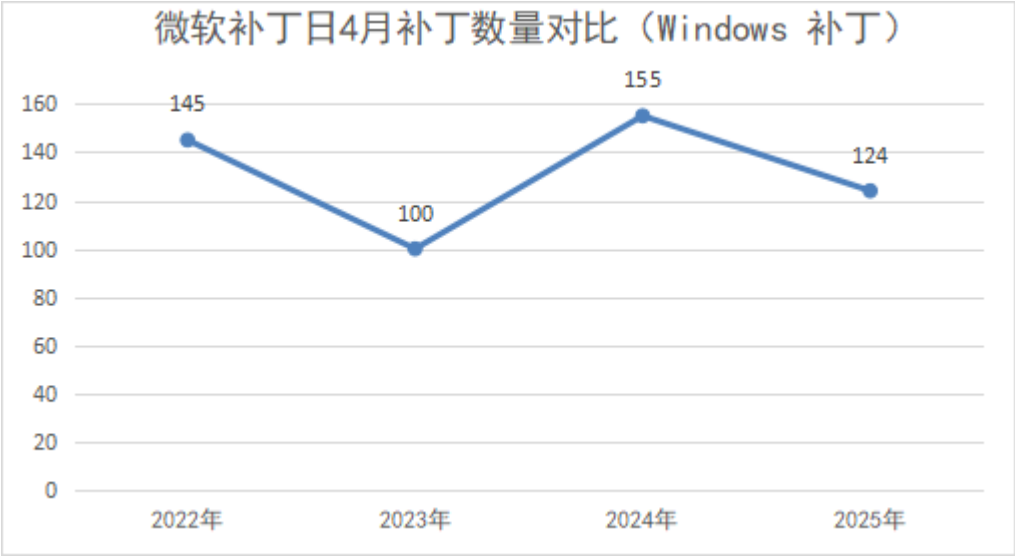



2025 年 4 月微软补丁漏洞修复情况

总体上来看，微软本月发布的补丁数量为 124 个，有 11 个 Critical 漏洞补丁。千里目安全技术中心在综合考虑往年微软公布漏洞数量的数据统计和今年的特殊情况，初步估计微软在今年五月份公布的漏洞数将比今年四月份少。漏洞数量将会维持在 80 个左右。

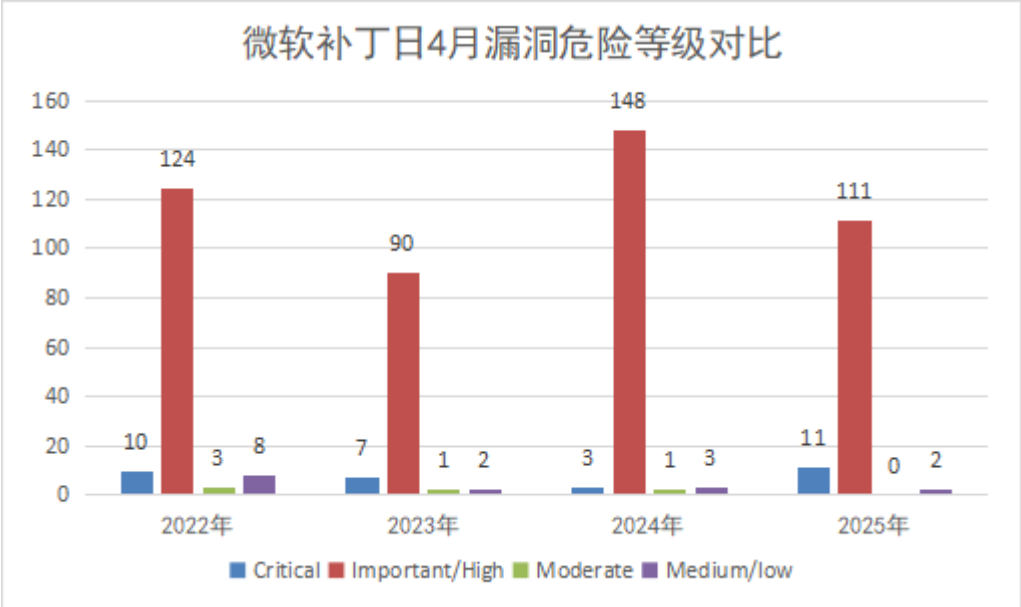
## 2 、历史微软补丁日 4 月漏洞对比

2022—2025 年，4 月份的 Windows 补丁趋势如下图：



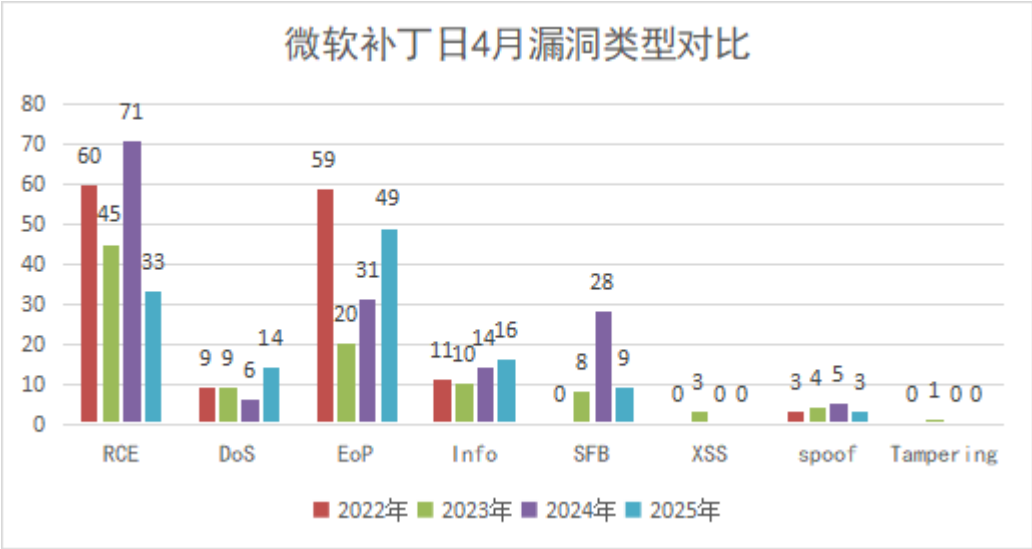

历年 4 月份微软 Windows 补丁趋势

2022-2025 年，4 月份的漏洞危险等级趋势和数量如下图：




历年 4 月份微软漏洞危险等级对比

2022-2025 年，4 月份的漏洞各个类型数量对比如下图：




微软近年 4 月漏洞类型对比

### 3、 漏洞数量分析

**从漏洞数量来看，今年相较去年减少**。微软在 2025 年 4 月份爆发的漏洞相较于去年减少。本月出现了 124 个漏洞补丁，并且有 11 个 Critical 类型的漏洞补丁。

**从漏洞的危险等级来看，相较去年“Critical”等级的漏洞数量增多，“Important/High”等级的漏洞数量减少。**本月出现了 11 个“Critical”等级的漏洞，相较去年增加了 267%；本月出现了 111 个“Important/High”等级的漏洞，相较去年减少了约 25%。

**从漏洞类型来看，RCE 类型的漏洞数量减少，DoS 类型的漏洞数量增多，EoP 类型的漏洞数量增多，**需要引起高度重视，尤其是 RCE 漏洞在配合社工手段的前提下，甚至可以直接接管整个局域网并进行进一步扩展攻击。

## （三） 重要漏洞分析

### 1、 漏洞分析

**Windows 通用日志文件系统驱动程序提升权限漏洞 CVE-2025-29824**

通用日志文件系统是一个通用目的的日志文件系统，它可以从内核模式或用户模式的应用程序访问，用以构建一个高性能的事务日志。

其中存在权限提升漏洞，攻击者可以利用该漏洞在目标系统获取更高的权限。该漏洞存在在野利用，经过评估，危害比较大，我们建议用户及时更新微软安全补丁。

**轻量级目录访问协议（LDAP）客户端远程代码执行漏洞 CVE-2025-26663**

轻量级目录访问协议（LDAP）是一种开放的工业标准协议，用于通过 IP 协议高效访问和维护分布式目录信息。它采用树形结构存储用户、权限等数据，支持快速查询和单点登录，广泛应用于企业内部系统、云服务及身份认证管理。

其中存在远程执行代码漏洞，攻击者可以利用该漏洞在目标系统执行任意代码，经过评估，危害比较大，我们建议用户及时更新微软安全补丁。

**轻量级目录访问协议（LDAP）客户端远程代码执行漏洞 CVE-2025-26670**

轻量级目录访问协议（LDAP）是一种开放的工业标准协议，用于通过 IP 协议高效访问和维护分布式目录信息。它采用树形结构存储用户、权限等数据，支持快速查询和单点登录，广泛应用于企业内部系统、云服务及身份认证管理。

其中存在远程执行代码漏洞，攻击者可以利用该漏洞在目标系统执行任意代码，经过评估，危害比较大，我们建议用户及时更新微软安全补丁。

## 2、 影响范围

| 漏洞名称/CVE | 受影响版本 |
| --- | --- |
| Windows 通用日志文件系统驱动程序提升权限漏洞 CVE-2025-29824 | Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 21H2 for 32-bit Systems<br>Windows 10 Version 21H2 for ARM64-based Systems<br>Windows 10 Version 21H2 for x64-based Systems<br>Windows 10 Version 22H2 for 32-bit Systems<br>Windows 10 Version 22H2 for ARM64-based Systems |

| | |
|---|---|
| | Windows 10 Version 22H2 for x64-based Systems<br>Windows 11 Version 22H2 for ARM64-based Systems<br>Windows 11 Version 22H2 for x64-based Systems<br>Windows 11 Version 23H2 for ARM64-based Systems<br>Windows 11 Version 23H2 for x64-based Systems<br>Windows 11 Version 24H2 for ARM64-based Systems<br>Windows 11 Version 24H2 for x64-based Systems<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for x64-based Systems Service Pack 2<br>Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2022<br>Windows Server 2022 (Server Core installation) |

| | |
|---|---|
| | Windows Server 2022, 23H2 Edition (Server Core installation)<br>Windows Server 2025<br>Windows Server 2025 (Server Core installation) |
| | Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 21H2 for 32-bit Systems<br>Windows 10 Version 21H2 for ARM64-based Systems<br>Windows 10 Version 21H2 for x64-based Systems<br>Windows 10 Version 22H2 for 32-bit Systems<br>Windows 10 Version 22H2 for ARM64-based Systems<br>Windows 10 Version 22H2 for x64-based Systems<br>Windows 11 Version 22H2 for ARM64-based Systems<br>Windows 11 Version 22H2 for x64-based Systems<br>Windows 11 Version 23H2 for ARM64-based Systems<br>Windows 11 Version 23H2 for x64-based Systems<br>Windows 11 Version 24H2 for ARM64-based Systems<br>Windows 11 Version 24H2 for x64-based Systems<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for x64-based Systems Service Pack 2 |

| | |
|---|---|
| Windows 轻量级目录访问协议（LDAP）远程代码执行漏洞 CVE-2025-26663 | Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2022<br>Windows Server 2022 (Server Core installation)<br>Windows Server 2022, 23H2 Edition (Server Core installation)<br>Windows Server 2025<br>Windows Server 2025 (Server Core installation) |
| 轻量级目录访问协议（LDAP）客户端远程代码执行漏洞 CVE-2025-26670 | Windows 10 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 21H2 for 32-bit Systems<br>Windows 10 Version 21H2 for ARM64-based Systems<br>Windows 10 Version 21H2 for x64-based Systems |

| | |
|---|---|
| | Windows 10 Version 22H2 for 32-bit Systems<br>Windows 10 Version 22H2 for ARM64-based Systems<br>Windows 10 Version 22H2 for x64-based Systems<br>Windows 11 Version 22H2 for ARM64-based Systems<br>Windows 11 Version 22H2 for x64-based Systems<br>Windows 11 Version 23H2 for ARM64-based Systems<br>Windows 11 Version 23H2 for x64-based Systems<br>Windows 11 Version 24H2 for ARM64-based Systems<br>Windows 11 Version 24H2 for x64-based Systems<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for x64-based Systems Service Pack 2<br>Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2019 (Server Core installation) |

| | |
|---|---|
| | Windows Server 2022<br>Windows Server 2022 (Server Core installation)<br>Windows Server 2022, 23H2 Edition (Server Core installation)<br>Windows Server 2025<br>Windows Server 2025 (Server Core installation) |

## 3 、修复建议

微软官方已更新受影响软件的安全补丁，用户可根据不同系统版本下载安装对应的安全补丁。

**安全更新链接如下：**

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26663

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26670

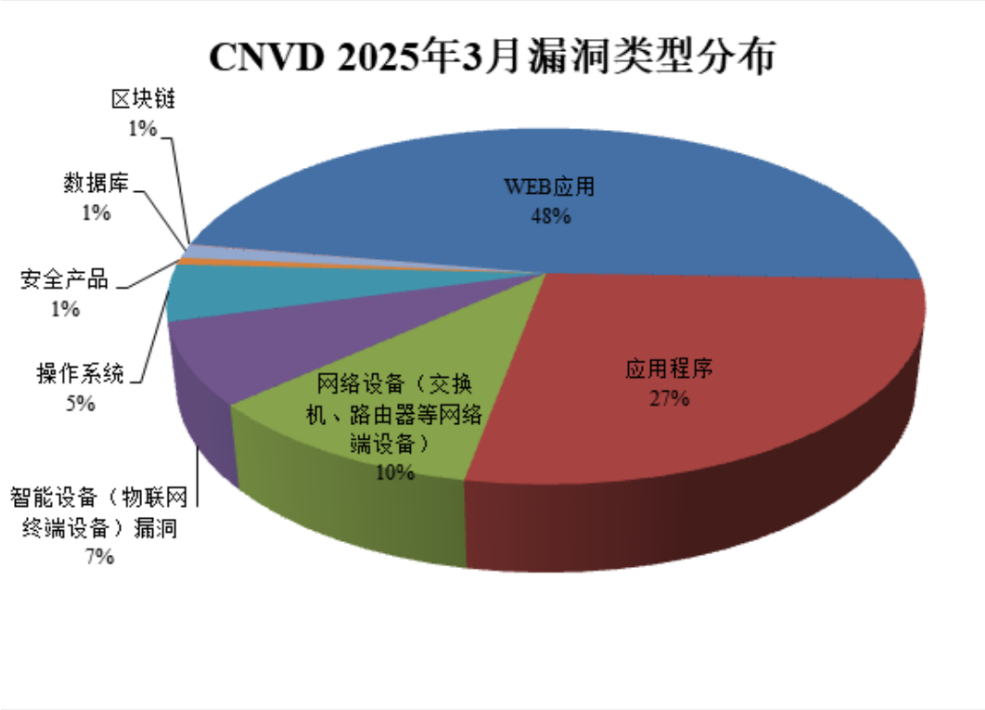
## 五、3 月份 CNVD 漏洞收录情况

国家信息安全漏洞共享平台（China National Vulnerability Database，以下简称 CNVD），3 月收集整理信息安全漏洞 1068 个，其中高危漏洞 459 个，中危漏洞 555 个，低危漏洞 54 个。

上述漏洞中，可被利用来实施远程网络攻击的漏洞有 841 个，数据来源自 CNVD 站点漏洞统计数据。

### （一）漏洞分类统计

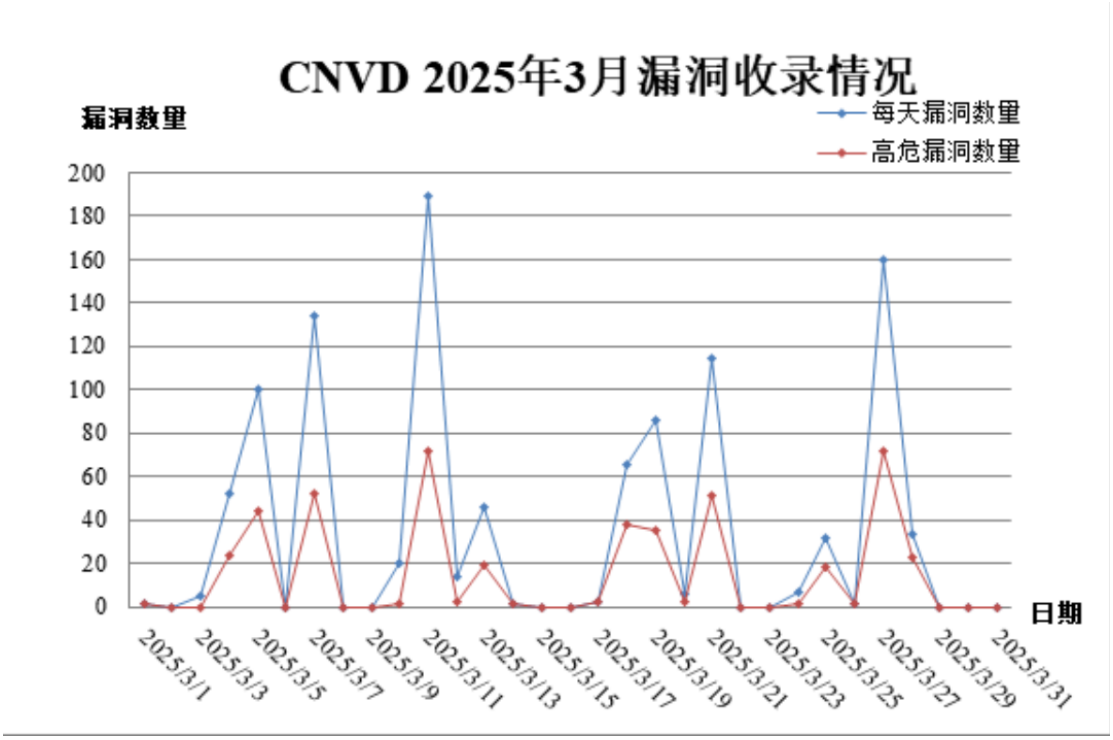
根据漏洞影响对象的类型，漏洞可分为 WEB 应用、应用程序、操作系统、网络设备（交换机、路由器等网络端设备）、数据库、安全产品（如防火墙、入侵检测系统等）、智能设备（物联网终端设备）和区块链漏洞。不同类型漏洞的分布如图 1 所示，3 月 WEB 应用占比例较大。与前 12 个月相比，智能设备（物联网终端设备）和区块链漏洞的数量处于高位，操作系统、应用程序、WEB 应用、网络设备（交换机、路由器等网络端设备）、数据库和安全产品漏洞的数量处于低位。




漏洞类型分布

## （二）漏洞趋势

3 月，CNVD 收集整理信息安全漏洞 1068 个，与前 12 个月平均收录数量 1481 个相比，处于低位；本月高危漏洞 459 个，与前 12 个月高危漏洞平均收录数量 711 个相比，处于低位。3 月的总体漏洞趋势如图所示




3 月份漏洞发布趋势

**附录：3 月份重要漏洞信息汇总**

3 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 | Linux 多款产品存在安全漏洞 | CNVD 编号 | CNVD-2025-04158、CNVD-2025-04157<br>CNVD-2025-04159、CNVD-2025-04164<br>CNVD-2025-04163、CNVD-2025-04162<br>CNVD-2025-04672、CNVD-2025-05380<br>CNVD-2025-05378、CNVD-2025-05382 | 3 月，Linux 多款产品存在安全漏洞。攻击者可利用漏洞造成内存破坏从而改变进程行为，造成拒绝服务，或利用进一步的漏洞来提升权限或执行任意代码等。3 月漏洞包括：Linux Kernel 内存破坏漏洞（CNVD-2025-04158、CNVD-2025-04157）、Linux Kernel 空指针解引用漏洞（CNVD-2025-04159、CNVD-2025-04164、CNVD-2025-04163、CNVD-2025-04162、CNVD-2025-05378、CNVD-2025-05382）、Linux kernel 内存错误引用漏洞（CNVD-2025-04672）、Linux kernel 竞争条件漏 |
| | | 其他编号 | CVE-2024-27072、CVE-2024-27041<br>CVE-2024-27037、CVE-2024-47809<br>CVE-2024-48881、CVE-2024-57798<br>CVE-2021-47653、CVE-2024-58087<br>CVE-2025-21848、CVE-2025-21854 | |
| | | 发布时间 | 2025-03-03 | |
| | | | Linux Kernel | |

| | | | | |
|---|---|---|---|---|
| | | 影响产品 | | 洞（CNVD-2025-05380）等。 |
| 2 | IBM 多款产品存在安全漏洞 | CNVD 编号 | CNVD-2025-04975、CNVD-2025-04976<br>CNVD-2025-04977、CNVD-2025-04978<br>CNVD-2025-05214、CNVD-2025-05217<br>CNVD-2025-05216、CNVD-2025-05389<br>CNVD-2025-05564、CNVD-2025-05563 | 3 月，IBM 多款产品存在安全漏洞。攻击者可利用漏洞暴力破解账户凭据，通过特制 URL 请求来查看系统上的任意文件，导致拒绝服务等。3 月漏洞包括：IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2025-04975、CNVD-2025-04976、CNVD-2025-04977、CNVD-2025-04978）、IBM Concert 暴力破解漏洞、IBM EntireX 路径遍历漏洞、IBM EntireX 拒绝服务漏洞、IBM MQ 拒绝服 |
| | | 其他编号 | CVE-2024-47116、CVE-2024-47103<br>CVE-2024-40696、CVE-2024-49807<br>CVE-2024-51476、CVE-2024-54169<br>CVE-2024-54170、CVE-2024-54175 | |

| | | | | |
|---|---|---|---|---|
| | | | CVE-2025-23225、CVE-2025-0975 | 务漏洞（CNVD-2025-05564）、IBM MQ 代码执行漏洞（CNVD-2025-05563、CNVD-2025-05389）等。 |
| | | **发布时间** | 2025-03-11 | |
| | | **影响产品** | IBM Sterling B2B Integrator<br>IBM Concert<br>IBM Entirex<br>IBM MQ | |
| 3 | **Microsoft 多款产品存在安全漏洞** | **CNVD 编号** | CNVD-2025-04189、CNVD-2025-04191<br>CNVD-2025-04192、CNVD-2025-04193<br>CNVD-2025-04194、CNVD-2025-04197<br>CNVD-2025-04198、CNVD-2025-05241<br>CNVD-2025-05243、CNVD-2025-05244 | 3 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。3 月漏洞包括：Microsoft Excel 代码执行漏洞（CNVD-2025-04189、CNVD-2025-04191、CNVD-2025-04192、CNVD-2025-04193、CNVD-2025-04194）、Microsoft Office 代码执行漏洞（CNVD-2025-04198、CNVD-2025-05243）、Microsoft Internet Explorer 代码执行漏洞、Microsoft Access 代码 |
| | | **其他编号** | CVE-2025-21354、CVE-2025-21386<br>CVE-2025-21387、CVE-2025-21390<br>CVE-2025-21394、CVE-2025-21395<br>CVE-2025-21392、CVE-2025-21326 | |

| | | | | |
|---|---|---|---|---|
| | | | CVE-2025-26629、CVE-2025-26630 | 执行漏洞（CNVD-2025-05244、CNVD-2025-04197）等。 |
| | | 发布时间 | 2025-03-05 | |
| | | 影响产品 | Microsoft Office Online Server<br>Microsoft Office LTSC for Mac 2024<br>Microsoft Office LTSC for Mac 2021<br>Microsoft Office LTSC 2021<br>Microsoft Office LTSC 2024<br>Microsoft Windows Server 2022<br>Microsoft Windows Server 2025<br>Microsoft 365 Apps for Enterprise<br>Microsoft Access 2016<br>Microsoft Excel 2016<br>Microsoft Office 2019<br>Microsoft Office 2016 | |
| 4 | | CNVD 编号 | CNVD-2025-05201、CNVD-2025-05200 | 3 月，Adobe 多款产品存在安全漏洞。攻击 |

| | | | | |
|---|---|---|---|---|
| | Adobe 多款产品存在安全漏洞 | | CNVD-2025-05202、CNVD-2025-05204<br>CNVD-2025-05208、CNVD-2025-05207<br>CNVD-2025-05210、CNVD-2025-05209<br>CNVD-2025-05212、CNVD-2025-05213 | 者可利用漏洞在当前用户的上下文中执行任意代码。3 月漏洞包括：Adobe Substance 3D Designer 越界写入漏洞（CNVD-2025-05201、CNVD-2025-05200、CNVD-2025-05202、CNVD-2025-05208、CNVD-2025-05209、CNVD-2025-05212、CNVD-2025-05213）、Adobe Substance 3D Designer 堆缓冲区溢出漏洞（CNVD-2025-05204、CNVD-2025-05207、CNVD-2025-05210）等。 |
| | | **其他编号** | CVE-2025-24450、CVE-2025-27172<br>CVE-2025-24451、CVE-2025-27173<br>CVE-2025-24444、CVE-2025-24443<br>CVE-2025-24439、CVE-2025-24440<br>CVE-2025-24441、CVE-2025-24445 | |
| | | **发布时间** | 2025-03-18 | |
| | | **影响产品** | Adobe Substance 3D Painter<br>Adobe Substance 3D Designer<br>Adobe Substance 3D Modeler<br>Adobe Substance 3D Sampler | |
| 5 | | | | |

| | | | | |
|---|---|---|---|---|
| | Apache 多款产品存在安全漏洞 | CNVD 编号 | CNVD-2025-04973、CNVD-2025-05169<br>CNVD-2025-05168、CNVD-2025-05699<br>CNVD-2025-05704、CNVD-2025-05703<br>CNVD-2025-05702、CNVD-2025-05706<br>CNVD-2025-05705、CNVD-2025-05994 | 3 月，Apache 多款产品存在安全漏洞。攻击者可利用漏洞获取敏感信息，执行跨站脚本攻击，并可能假冒其他用户，执行恶意代码获取服务器权限等。3 月漏洞包括：Apache Tomcat 远程代码执行漏洞、Apache Camel 任意命令执 漏洞（CNVD-2025-05168、CNVD-2025-05169）、Apache EventMesh 反序列化漏洞（CNVD-2025-05699）、Apache Doris 路径遍历漏洞、Apache Hive 授权问题漏洞、Apache Hive 信任管理问题漏洞、Apache Atlas 跨站脚本漏洞（CNVD-2025-05706）、Apache James 资源管理错误漏洞、Apache Hadoop 授权问题漏洞（CNVD-2025-05994）等。 |
| | | 其他编号 | CVE-2025-24813、CVE-2025-27636<br>CVE-2025-29891、CVE-2024-56180<br>CVE-2024-48019、CVE-2024-29869<br>CVE-2024-23953、CVE-2024-46910<br>CVE-2024-45626、CVE-2024-23454 | |
| | | 发布时间 | 2025-03-25 | |
| | | 影响产品 | Apache Software Foundation<br>Apache Tomcat<br>Apache Camel<br>Apache EventMesh<br>Apache Doris<br>Apache Hive | |

| | | | | |
|---|---|---|---|---|
| | | | Apache Atlas<br>Apache James<br>Apache Hadoop | |
| 6 | Cisco 多款产品存在安全漏洞 | CNVD 编号 | CNVD-2025-05709、CNVD-2025-05712<br>CNVD-2025-05711、CNVD-2025-05933<br>CNVD-2025-05931、CNVD-2025-05934<br>CNVD-2025-05946、CNVD-2025-05983<br>CNVD-2025-05984、CNVD-2025-05985 | 3 月，Cisco 多款产品存在安全漏洞。攻击者可利用漏洞导致信息泄露，可以对该界面的用户发起反射型跨站脚本（XSS）攻击，获得设备上的 root 访问权限等。3 月漏洞包括：Cisco IOS XR Software CLI 本地权限提升漏洞、Cisco Meraki MX67 和 Cisco Meraki MX68 访问验证错误漏洞、Cisco Content Security Management Appliance 访问验证错误漏洞、Cisco Application Policy Infrastructure Controller CLI 存在命令注入漏洞、Cisco TelePresence Managem |
| | | 其他编号 | CVE-2025-20138、CVE-2019-1815<br>CVE-2020-3122、CVE-2025-20117<br>CVE-2025-20208、CVE-2025-20211<br>CVE-2025-20153、CVE-2024-20445<br>CVE-2024-20512、CVE-2024-20370 | |
| | | 发布时间 | 2025-03-24 | |

| | | | | |
|---|---|---|---|---|
| | | **影响产品** | Cisco IOS XR Software CLI<br>Cisco Meraki MX67<br>Cisco Meraki MX68<br>Cisco Content Security Management Appliance<br>Cisco Application Policy Infrastructure Controller (APIC)<br>Cisco TelePresence Management Suite<br>Cisco BroadWorks Application Delivery Platform<br>Cisco Secure Email Gateway<br>Cisco Desk Phone 9800<br>Cisco IP Phone 7800<br>Cisco IP Phone 8800<br>Cisco Video Phone 8875<br>Cisco Unified Contact Center Management Portal<br>Cisco Firepower Threat Defense | ent Suite 跨站脚本漏洞、Cisco BroadWorks Application Delivery Platform 跨站脚本漏洞、Cisco Secure Email Gateway 访问控制错误漏洞、Cisco IP Phone 信息泄露漏洞、Cisco Unified Contact Center Management Portal 跨站脚本漏洞、Cisco Firepower Threat Defense 和 Cisco Adaptive Security Appliance 授权问题漏洞等。 |

| | | | | |
|---|---|---|---|---|
| | | | Cisco Adaptive Security Appliance | |
| 7 | Google 多款产品存在安全漏洞 | CNVD 编号 | CNVD-2025-05085、CNVD-2025-05084CNVD-2025-05088、CNVD-2025-05087CNVD-2025-05089、CNVD-2025-05092CNVD-2025-05091、CNVD-2025-05093CNVD-2025-05219、CNVD-2025-05218 | 3 月，Google 多款产品存在安全漏洞。攻击者可利用漏洞绕过安全限制，提升权限，在系统上执行任意代码等。3 月漏洞包括：Google Chrome 代码执行漏洞（CNVD-2025-05085、CNVD-2025-05084、CNVD-2025-05087、CNVD-2025-05092、CNVD-2025-05091）、Google Android 权限提升漏洞（CNVD-2025-05219、CNVD-2025-05218）、Google Chrome 安全绕过漏洞（CNVD-2025-05088、CNVD-2025-05089、CNVD-2025-05093）等。 |
| | | 其他编号 | CVE-2025-2135、CVE-2025-1920<br>CVE-2025-0440、CVE-2025-2136<br>CVE-2025-0435、CVE-2025-0439<br>CVE-2025-0436、CVE-2025-0446<br>CVE-2024-34748、CVE-2024-40669 | |
| | | 发布时间 | 2025-03-14 | |
| | | 影响产品 | Google Chrome<br>Google Android | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| 8 | Esri 多款产品存在安全漏洞 | CNVD 编号 | CNVD-2025-05054、CNVD-2025-05055CNVD-2025-05056、CNVD-2025-05057CNVD-2025-05058、CNVD-2025-05059CNVD-2025-05060、CNVD-2025-05061CNVD-2025-05079、CNVD-2025-05082 | 3 月，Esri 多款产品存在安全漏洞。攻击者可利用漏洞访问安全服务，查看、添加、修改或删除后端数据库中的信息等。3 月漏洞包括：Esri ArcGIS Server 跨站脚本漏洞（CNVD-2025-05055、CNVD-2025-05056、CNVD-2025-05057、CNVD-2025-05058、CNVD-2025-05059、CNVD-2025-05060、CNVD-2025-05061）、Esri ArcGIS Server 访问控制错误漏洞、Esri ArcGIS Server 文件包含漏洞、Esri ArcGIS Server SQL 注入漏洞（CNVD-2025-05054）等。 |
| | | 其他编号 | CVE-2024-51962、CVE-2024-10904 CVE-2024-51942、CVE-2024-51944 CVE-2024-51945、CVE-2024-51947 CVE-2024-51948、CVE-2024-51949 CVE-2024-51954、CVE-2024-51961 | |
| | | 发布时间 | 2025-03-12 | |
| | | 影响产品 | ESRI ArcGIS Server | |