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 月上）

深信服科技股份有限公司

2025 年 5 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 5 月份（5.5-5.20）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 F5 BIG-IP Appliance 模式命令执行漏洞、Ivanti EPMM 未授权远程代码执行，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、人民银行近日发布《中国人民银行业务领域数据安全管理办法》

2、国务院 2025 年预备制定网络安全等级保护条例

国际政策法规：

1、英国国家网络安全中心(NCSC)推出网络弹性设施和威胁模拟计划

2、泰国培训十万网络安全人员打击网络犯罪

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、人民银行近日发布《中国人民银行业务领域数据安全管理办法》

5 月 9 日，为贯彻党中央、国务院关于数据安全的决策部署，落实《中华人民共和国数据安全法》，进一步夯实数据安全的法治基础，指导督促金融从业机构依法依规开展中国人民银行业务领域数据（以下简称“业务数据”）处理活动，中国人民银行发布《中国人民银行业务领域数据安全管理办法》（以下简称《办法》），自 2025 年 6 月 30 日起施行。

该《办法》旨在规范金融业务领域数据全生命周期安全管理，平衡数据开发利用与风险防控，覆盖货币信贷、支付清算、征信、反洗钱等十大央行监管业务领域 157。核心内容包括：分类分级管理，将数据分为一般、重要、核心三级，其中核心数据若被非法使用可能直接影响政治安全，需最高级别保护；全流程管控，要求高敏感数据原则上不得导出或脱敏展示，限制生物识别信息收集场景，并规范数据收集、存储、使用、传输等环节 157；技术防护强化，明确核心数据系统需达到四级网络安全标准，数据传输加密，禁止通过互联网随意传输高敏感数据；主体责任落实，遵循“谁管业务谁管数据安全”原则，要求金融机构每年更新数据资源目录，配备安全专业人员并开展年度培训；风险应急机制，强制重要数据处理者每年开展安全评估，重大数据事件需 24 小时内启动应急响应并报告 15。该政策通过制度与技术协同筑牢金融数据安全防线，保障个人隐私与国家安全，促进数据依法有序流动，为金融业数字化转型提供制度支撑。

原文链接：

央行发布《中国人民银行业务领域数据安全管理办法》

2、国务院 2025 年预备制定网络安全等级保护条例

5 月 14 日消息，国务院办公厅印发《国务院 2025 年度立法工作计划》，其中多项内容和网络与信息安全相关，包括制定政务数据共享条例，预备制定网络安全等级保护条例、终端设备直连卫星服务管理条例，预备修订政府信息公开条例、互联网信息服务管理办法、反间谍法实施细则，推进人工智能健康发展立法工作。

此前公安部于 2018 年 6 月公布《网络安全等级保护条例（征求意见稿）》对外公开征求意见，时隔 7 年后，该文件终于迎来新进展。

原文链接：

国务院办公厅关于印发《国务院 2025 年度立法工作计划》的通知_国务院文件_中国政府网

全球瞭望｜网络安全重大事件精选（168 期）

（二）国际政策法规：

1、英国国家网络安全中心(NCSC)推出网络弹性设施和威胁模拟计划

近日，英国政府通信总部下属国家网络安全中心（NCSC）公布了两项旨在增强英国国家网络弹性的关键举措，并增强公共和私营部门的网络防御能力。一是构建全国性的网络弹性测试设施（CRTF），使技术供应商能验证产品抗攻击能力，重点保障关键基础设施供应链安全，首批设施将于今夏投入运营；二是构建网络对手模拟（CyAS）计划，通过红队演练帮助各组织评估并增强其检测响应网络威胁的能力，初期覆盖政府及能源、金融等关键行业。

原文链接：

全球瞭望｜网络安全重大事件精选（168 期）

2、泰国培训十万网络安全人员打击网络犯罪

当地时间 5 月 5 日，由泰国国家网络安全局组织的网络安全培训班举行结业仪式，泰国副总理兼国防部长普坦主持结业仪式。10 万名来自各行各业的网络安全人员完成培训任务，此举将会提升泰国网络安全工作能力。泰国副总理兼数字经济与社会部部长巴瑟在结业仪式上表示，随着泰国迈入全面数字化时代，网络安全在建立信任方面发挥着关键作用。“泰国优先发展数字基础设施，以推动可持续的经济、社会和国家安全。”巴瑟说，必须加强各机构间的合作，应对国际网络威胁，打击网络犯罪，包括电信诈骗和网络赌博。

原文链接：

国际 | 泰国培训十万网络安全人员打击网络犯罪

二、安全热点时事资讯

（一）国内安全事件

广州某科技公司遭网络攻击，锁定为境外“黑手”

时间：5 月 20 日

概况：上午 9 时，广东省广州市公安局天河区分局发布警情通报称，广州某科技公司自助设备的后台系统遭受网络攻击并被上传多份恶意代码。接警后，公安机关立即开展调查，提取相关样本，依法固定电子证据。经对网络攻击手法和相关恶意代码样本开展技术分析，现已初步判定该事件为境外黑客组织发起的网络攻击活动。

据警方透露，此次网络攻击是境外黑客组织的一次有组织、有预谋的大规模网络攻击行动，带有明显的网络战痕迹并非普通个人黑客所能完成。初步追踪溯源发现，该黑客组织长期使用开源工具对我重要部门、敏感行业和科技公司开展网络资产扫描探测，广泛搜寻攻击目标，通过技术手段挖掘目标单位网络防护薄弱环节和攻击点位，伺机入侵控制目标系统，窃取、破坏重要数据。

安全防御建议：

- 纵深防御体系：部署多层次防护（如入侵检测、行为分析），并定期进行红蓝对抗演练，发现潜在漏洞。
- 溯源与威胁情报：建立攻击样本库，结合威胁情报分析攻击手法，提升主动防御能力。
- 国际合作反制：针对境外 APT 攻击，需加强跨国执法协作与技术共享，形成联合反制机制。

原文链接：

广州某科技公司遭网络攻击，境外“黑手”被锁定

（二）国际安全事件

1、时尚巨头迪奥遭遇网络攻击导致客户信息外泄事件

时间：5 月 7 日

概况：法国奢侈品牌迪奥（Dior）发现其时尚与配饰客户数据库遭到未授权访问，导致包括中国和韩国在内的多个国家的客户个人信息泄露。此次事件引发了全球对奢侈品牌数据安全和数字信任的广泛关注。迪奥表示，受影响的数据包括客户的姓名、性别、电话号码、电子邮件地址、邮寄地址、购物偏好和购买历史等。幸运的是，账户密码和支付信息（如银行账户或信用卡信息）存储在不同的数据库中，未受到此次事件的影响。

在中国，迪奥于 5 月 12 日通过短信通知受影响的客户，并向媒体致歉，强调客户数据的保密性和安全性始终是其首要任务。公司已向相关监管机构报告此事件，并与网络安全专家合作进行调查。

安全防御建议：

- 数据分类与隔离：敏感数据（如支付信息）应物理或逻辑隔离存储，降低单点泄露风险。

- 合规与透明沟通：遵循《通用数据保护条例》（GDPR）等法规，确保数据泄露后及时向监管机构和用户通报，避免法律风险。
- 供应链安全：第三方服务商或分支机构可能成为攻击入口，需纳入整体安全评估范围。

原文链接：

时尚巨头迪奥发生大规模数据泄漏，包括高价值中国客户资料

2、攻击团伙对美国知名教育科技服务商 PowerSchool 实施多重勒索

时间：5 月 7 日

概况：美国知名教育科技服务商 PowerSchool 证实，去年年底曾遭受勒索攻击并支付了数百万美元赎金，但攻击者并未删除数据。相反，黑客近日又发起新一轮勒索，直接向 PowerSchool 合作的 20 余家教育机构索要赎金，威胁公开所窃取的学生与职工敏感信息。

安全防御建议：

- 避免支付赎金：赎金无法保证数据安全，反而可能助长重复勒索，应优先通过备份恢复数据并与执法部门合作。
- 强化凭证管理：采用多因素认证（MFA）和零信任架构，防止凭证泄露导致横向渗透。
- 数据泄露预案：制定包含信用监控、法律支持和公众沟通的应急计划，减少声誉损失。
- 主动防御：从被动响应转向主动监测，利用 AI 和态势感知技术预测攻击路径。

原文链接：

攻击团伙实施多重勒索，美国知名教育科技服务商 PowerSchool 支付数百万赎金后，其合作的二十余家教育机构再遭勒索

3、印巴冲突中巴方攻击“致印度 70%电网瘫痪”事件

时间：5 月 10 日

概况：巴基斯坦军方宣称通过代号“铜墙铁壁”的军事行动对印度电网发动网络攻击，导致印度约 70%电网瘫痪。攻击手段包括利用钓鱼邮件或供应链漏洞渗透电力调度控制系统（SCADA），发送恶意指令断开断路器，并结合 DDoS 攻击使监控平台崩溃，引发多地停电及连锁社会危机。印度官方否认此说法，但媒体报道称多个地区确实出现停电，专家认为攻击可能导致电力系统连锁故障。

安全防御建议：

- 关键基础设施防护：电力、能源等关基设施需强化“安全分区、网络专用、横向隔离”的防护架构，定期更新老旧系统并严格隔离 IT/OT 网络。
- 应急响应能力：建立动态防御体系，包括态势感知、备用电源和快速恢复机制，以应对可能的雪崩效应。
- 国际合作与法规遵循：参考中国《关键信息基础设施安全保护条例》，落实“三同步”原则（安全与建设同步规划、实施、使用），加强跨境网络安全协作。

原文链接：

巴方攻击“致印度 70%电网瘫痪”是真是假？最新解读来了

巴方启动“铜墙铁壁”军事行动，“致印度约 70%电网瘫痪” 财经头条

【国家要害】印巴冲突中印度电网瘫痪事件对中国的启示与借鉴

（三）国际安全热点

1、2025 年汽车行业已发生勒索攻击 70 余起，新能源汽车供应链沦为攻击靶心

据 5 月 7 日报道，以色列汽车网络安全公司 Upstream Security 发布《2025

年全球汽车和智能出行网络安全报告》。分析显示，2025 年第一季度，全球汽车行业共发生 148 起网络安全事件，其中勒索软件攻击事件 70 余起，占比高达 45%，成为行业头号网络安全威胁。与此同时，针对新能源汽车的攻击事件频发，引发了业务中断、数据泄露，甚至远程控制车辆等风险。

原文链接：

2025 年汽车行业已发生勒索攻击 70 余起，新能源汽车供应链沦为攻击靶心

2、RSAC 2025 盘点：网络安全主战场已锁定 AI 安全

RSAC 2025 用一系列硬核数据击碎了“AI 仅是锦上添花”的误解：防护曲线止跌回升不是因为引入了花哨的新名词，而是因为 CISO 们真正在日常运营里把自动化、模型治理、合规留痕做到了位。未来 12 个月，Agentic AI 将迎来验证期——能否持续压缩驻留时间、进一步提升 61%的有效线，才是“下一站增长点”能否兑现的关键。对于每一位安全从业者而言，AI 不再是可选模块，而是必须铸进系统底座的工程学现实。 本文复盘了 RSAC 2025 中几个关键信息 。

原文链接：

RSAC 2025 盘点：网络安全主战场已锁定 AI 安全

三、安全风险通告

（一） F5 BIG-IP Appliance 模式命令执行漏洞(CVE-2025-31644)

漏洞名称 ：F5 BIG-IP Appliance 模式命令执行漏洞(CVE-2025-31644)

漏洞描述：2025 年 5 月 13 日，深瞳漏洞实验室监测到一则 F5-BIG-IP 组件存在命令执行漏洞的信息。当 F5 BIG-IP 运行在 Appliance 模式时，TMOS Shell（tmsh）中存在一个命令执行漏洞，**具有管理员角色的认证攻击者可以利用该漏洞执行任意系统命令，导致服务器失陷**。

漏洞编号：CVE-2025-31644，漏洞威胁等级：**高危**。

组件介绍：

F5 BIG-IP 是由 F5 Networks 公司开发和提供的一种高级的应用交付控制器（Application Delivery Controller，ADC）和负载均衡设备。它是一款广泛用于大型企业和数据中心环境的网络设备，用于提高应用程序性能、可用性、安全性和可扩展性。

影响范围：

目前受影响的 F5-BIG-IP 版本：

17.1.0 ≤ F5 BIG-IP < 17.1.2.2

16.1.0 ≤ F5 BIG-IP < 16.1.6

15.1.0 ≤ F5 BIG-IP < 15.1.10.7

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>：困难，需要管理员权限。

<综合评定威胁等级>：高危，能造成远程命令执行。

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 F5 BIG IP 更新到以下版本：

F5 BIG-IP 17.1.2.2

F5 BIG-IP 16.1.6

F5 BIG-IP 15.1.10.7

链接如下：

https://my.f5.com/manage/s/article/K000148591

深信服解决方案：

1、漏洞安全监测

支支持对 F5 BIG-IP Appliance 模式命令执行漏洞(CVE-2025-31644)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】预计 2025 年 05 月 21 日发布监测方案，规则 ID:11029220。

【深信服安全托管服务 MSS】预计 2025 年 05 月 21 日发布监测方案（需要具备 SIP 组件能力），规则 ID:11029220。

【深信服安全检测与响应平台 XDR】预计 2025 年 05 月 21 日发布监测方案，规则 ID:11029220。

2、漏洞安全防护

支持对 F5 BIG-IP Appliance 模式命令执行漏洞(CVE-2025-31644)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】预计 2025 年 05 月 21 日发布防护方案，规则 ID:11029220。

【深信服 Web 应用防火墙 WAF】预计 2025 年 05 月 21 日发布防护方案，规则 ID:11029220。

【深信服安全托管服务 MSS】预计 2025 年 05 月 21 日发布防护方案（需要具备 AF 组件能力），规则 ID:11029220。

【深信服安全检测与响应平台 XDR】预计 2025 年 05 月 21 日发布防护方案（需要具备 AF 组件能力），规则 ID:11029220。

（二） Ivanti EPMM 未授权远程代码执行(CVE-2025-4428)

漏洞名称 ：Ivanti EPMM 未授权远程代码执行(CVE-2025-4428)

漏洞描述： 2025 年 5 月 16 日，深瞳漏洞实验室监测到一则 Ivanti-Endpoint-Manager-Mobile 组件存在代码执行漏洞的信息。Ivanti Endpoint Manager Mobile 存在一个远程代码执行漏洞，**未授权的攻击者可以利用 CVE-2025-4427 和 CVE-2025-4428 在目标系统执行任意代码，导致服务器失陷。注：该漏洞已存在攻击代码披露**。

漏洞编号：CVE-2025-4428，漏洞威胁等级：**高危**。

组件介绍：

Ivanti Endpoint Manager Mobile 是一款移动设备管理（MDM）软件，旨在帮助企业管理其员工使用的移动设备。它可以帮助企业管理和保护移动设备、应用程序和数据，以确保企业数据的安全性和合规性。Ivanti Endpoint Manager Mobile 可以管理各种移动设备，包括 iOS、Android 和 Windows 设备。它提供了一系列功能，包括设备配置、应用程序管理、数据保护、网络访问控制、远程锁定和擦除等。

影响范围：

目前受影响的 Ivanti-Endpoint-Manager-Mobile 版本：

11.0.0.0 ≤ Ivanti EPMM < 11.12.0.5

12.3.0.0 ≤ Ivanti EPMM < 12.3.0.2

12.4.0.0 ≤ Ivanti EPMM < 12.4.0.2

Ivanti EPMM 12.5.0.0

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，无需授权即可造成远程代码执行。

<综合评定威胁等级>：高危，能造成远程代码执行。

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 Ivanti EPMM 更新到以下版本：

Ivanti EPMM 11.12.0.5

Ivanti EPMM 12.3.0.2

Ivanti EPMM 12.4.0.2

Ivanti EPMM 12.5.0.1

链接如下：

https://forums.ivanti.com/s/product-downloads

深信服解决方案：

1、漏洞主动检测

支持对 Ivanti EPMM 未授权远程代码执行(CVE-2025-4428)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】 已发布资产检测方案，规则 ID:SF-2025-00478。

【深信服漏洞评估工具 TSS】已发布资产检测方案，规则 ID:SF-2025-00987。

【深信服安全托管服务 MSS】已发布资产检测方案（需要具备 TSS 组件能力），规则 ID:SF-2025-00987。

【深信服安全检测与响应平台 XDR】已发布资产检测方案（需要具备云镜组件能力），规则 ID:SF-2025-00478。

2、漏洞安全监测

支持对 Ivanti EPMM 未授权远程代码执行(CVE-2025-4428)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】预计 2025 年 05 月 26 日发布监测方案，规则 ID:11029228。

【深信服安全托管服务 MSS】预计 2025 年 05 月 26 日发布监测方案（需要具备 SIP 组件能力），规则 ID:11029228。

【深信服安全检测与响应平台 XDR】预计 2025 年 05 月 26 日发布监测方案，规则 ID:11029228。

3、漏洞安全防护

支持对 Ivanti EPMM 未授权远程代码执行(CVE-2025-4428)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】预计 2025 年 05 月 26 日发布防护方案，规则 ID:11029228。

【深信服 Web 应用防火墙 WAF】预计 2025 年 05 月 26 日发布防护方案，规则 ID:11029228。

【深信服安全托管服务 MSS】预计 2025 年 05 月 26 日发布防护方案（需要具备 AF 组件能力），规则 ID:11029228。

【深信服安全检测与响应平台 XDR】预计 2025 年 05 月 26 日发布防护方案（需要具备 AF 组件能力），规则 ID:11029228。

四、微软安全通告

（一） 漏洞概要

2025 年 5 月 14 日（北京时间），微软发布了 2025 年 5 月安全更新，共发布了 82 个 CVE 的补丁程序，同比上月减少了 42 个。

在漏洞安全等级方面，存在 11 个标记等级为“Critical”的漏洞，67 个漏洞被标记为“Important/High”等级的漏洞； 在漏洞类型方面，主要有 32 个远程代码执行漏洞，21 个权限提升漏洞以及 17 个信息泄露漏洞。

（二） 漏洞数据分析

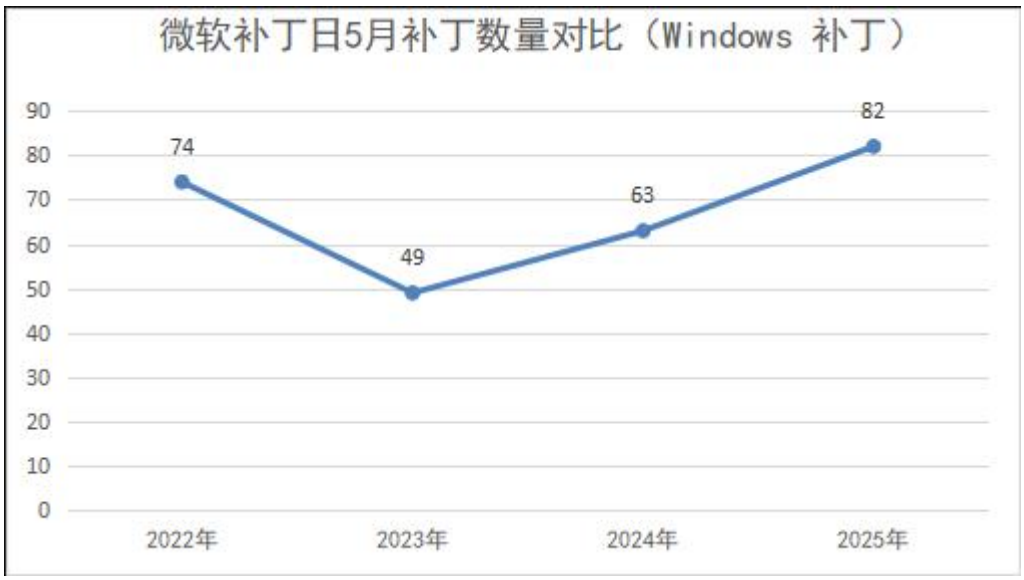
1、 漏洞数量趋势

近一年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 82 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六月份公布的漏洞数将比今年五月份少。漏洞数量将会维持在 70 个左右。

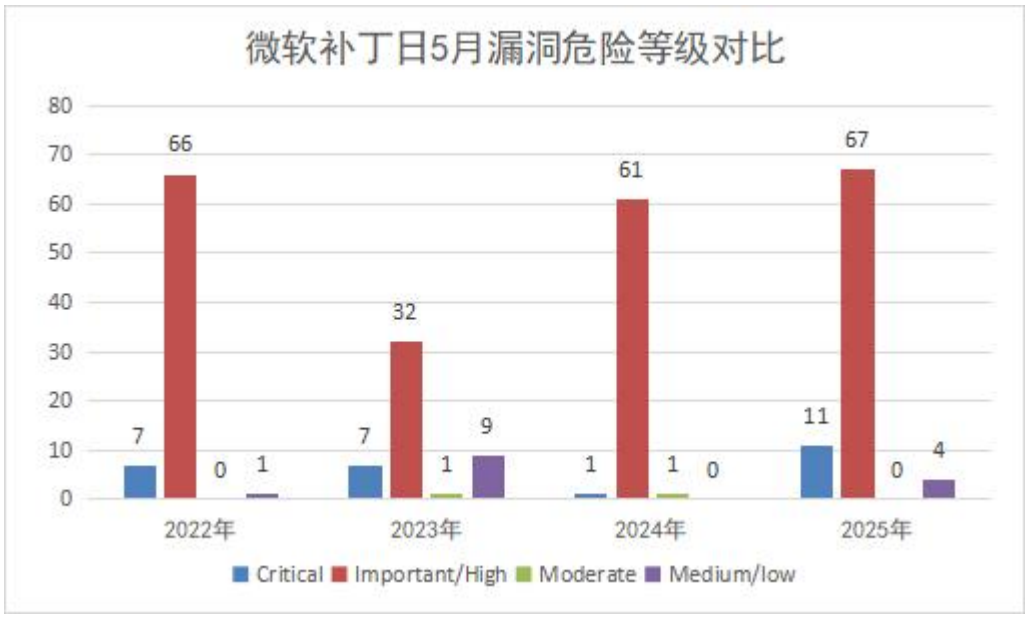
2 、历史微软补丁日 5 月漏洞对比

2022—2025 年，5 月份的 Windows 补丁趋势如下图：



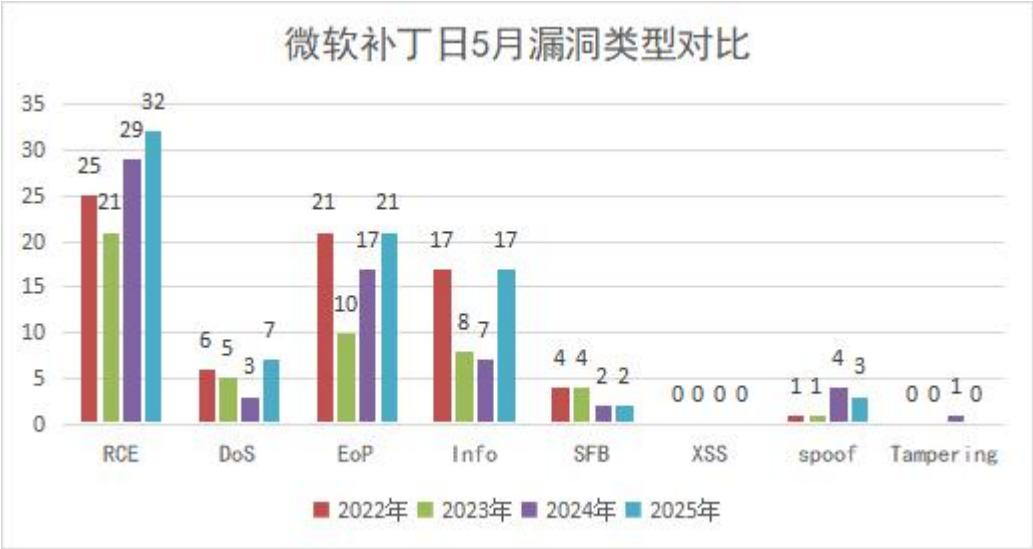
历年 5 月份微软 Windows 补丁趋势

2022-2025 年，5 月份的漏洞危险等级趋势和数量如下图：



历年 5 月份微软漏洞危险等级对比

2022-2025 年，5 月份的漏洞各个类型数量对比如下图：



微软近年 5 月漏洞类型对比

3、 漏洞数量分析

从漏洞数量来看，今年相较去年增多。微软在 2025 年 5 月份爆发的漏洞相较于去年增多。本月出现了 82 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 1000%；本月出现了 67 个“Important/High”等级的漏洞，相较去年减少了约 10%。

从漏洞类型来看，RCE 类型的漏洞数量增多，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

Microsoft DWM 核心库权限提升漏洞 CVE-2025-30400

DWM 桌面窗口管理器是自 Windows Vista 以来 Microsoft Windows 中的合成窗口管理器，它允许使用硬件加速来呈现 Windows 的图形用户界面。它最初是

为了启用部分新的“ Windows Aero ”用户体验而创建的，它允许诸如透明度、3D 窗口切换等效果。

其中存在特权提升漏洞，攻击者可以利用该漏洞在目标系统上获取更高的权限。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。

脚本引擎内存损坏漏洞 CVE-2025-30397

脚本引擎负责解析如 Javascript 等的脚本。在 MSHTML, EdgeHTML 和脚本平台中使用，Microsoft Edge 中的 Internet Explorer 模式以及使用 WebBrowser 控件的其他应用程序使用 MSHTML 平台。WebView 和一些 UWP 应用程序使用 EdgeHTML 平台。MSHTML 和 EdgeHTML 使用脚本平台。

其中存在内存损坏漏洞，可导致远程执行代码攻击，攻击者可以利用该漏洞在目标系统执行任意代码，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。

WinSock 的 Windows 辅助功能驱动程序特权提升漏洞 CVE-2025-32709

Winsock 是 Windows 操作系统的网络编程接口，定义了应用程序如何通过套接字访问网络服务，特别是 TCP/IP 协议。它提供了标准接口，使得 Windows 上的网络应用程序能够进行数据传输和通信。

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。

Windows 通用日志文件系统驱动程序提升权限漏洞 CVE-2025-32701 CVE-2025-32706

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。

2、 影响范围

漏洞名称/CVE	受影响版本
Microsoft DWM 核心库权限提升漏洞 CVE-2025-30400	Windows Server 2025 (Server Core installation) Windows Server 2025 Windows Server 2022, 23H2 Edition (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems
	Windows Server 2025 (Server Core installation) Windows Server 2025 Windows Server 2022, 23H2 Edition (Server Core installation)

脚本引擎内存损坏漏洞 CVE-2025-30397	Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems

	Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems
WinSock 的 Windows 辅助功能驱动程序特权提升漏洞 CVE-2025-32709	Windows Server 2025 (Server Core installation) Windows Server 2025 Windows Server 2022, 23H2 Edition (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems

	Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems
Windows 通用日志文件系统驱动程序提升权限漏洞 CVE-2025-32701、CVE-2025-32706	Windows Server 2025 (Server Core installation) Windows Server 2025 Windows Server 2022, 23H2 Edition (Server Core installation) Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Serv

	ice Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems

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-2025-30400

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30397

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32709

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32701

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32706

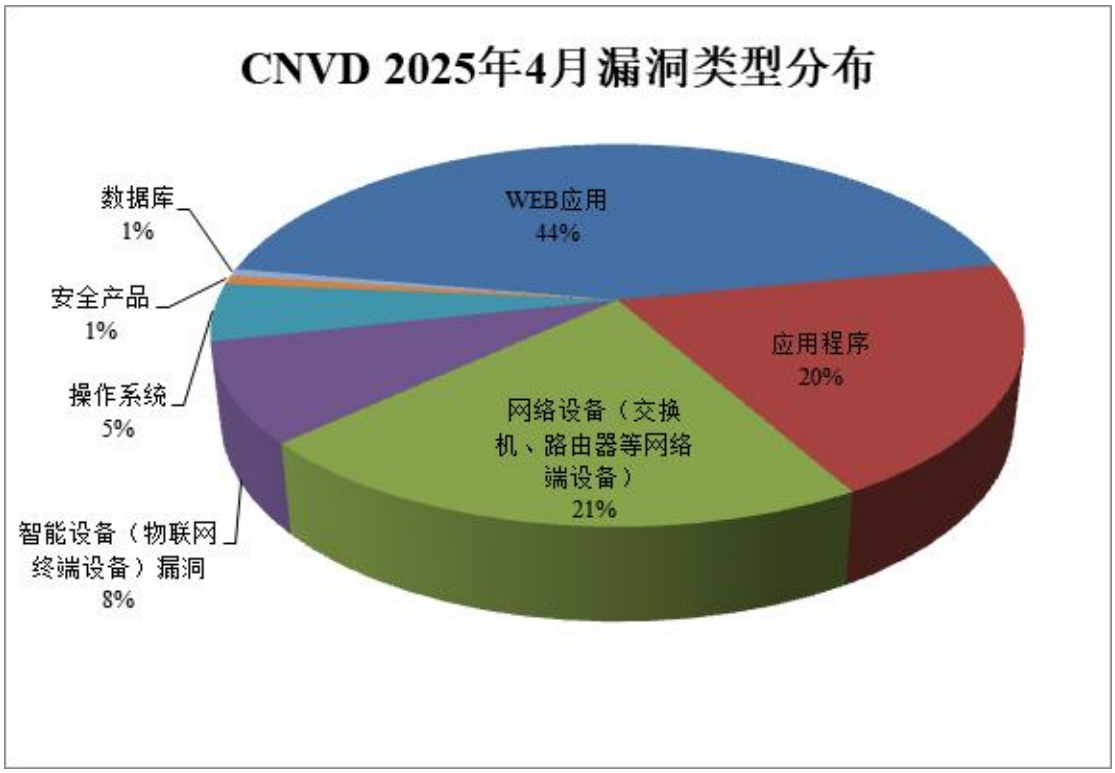
五、4 月份 CNVD 漏洞收录情况

国家信息安全漏洞共享平台（China National Vulnerability Database，以下简称 CNVD），4 月收集整理信息安全漏洞 1554 个，其中高危漏洞 780 个，中危漏洞 685 个，低危漏洞 89 个。

上述漏洞中，可被利用来实施远程网络攻击的漏洞有 1340 个，数据来源自 CNVD 站点漏洞统计数据。

（一）漏洞分类统计

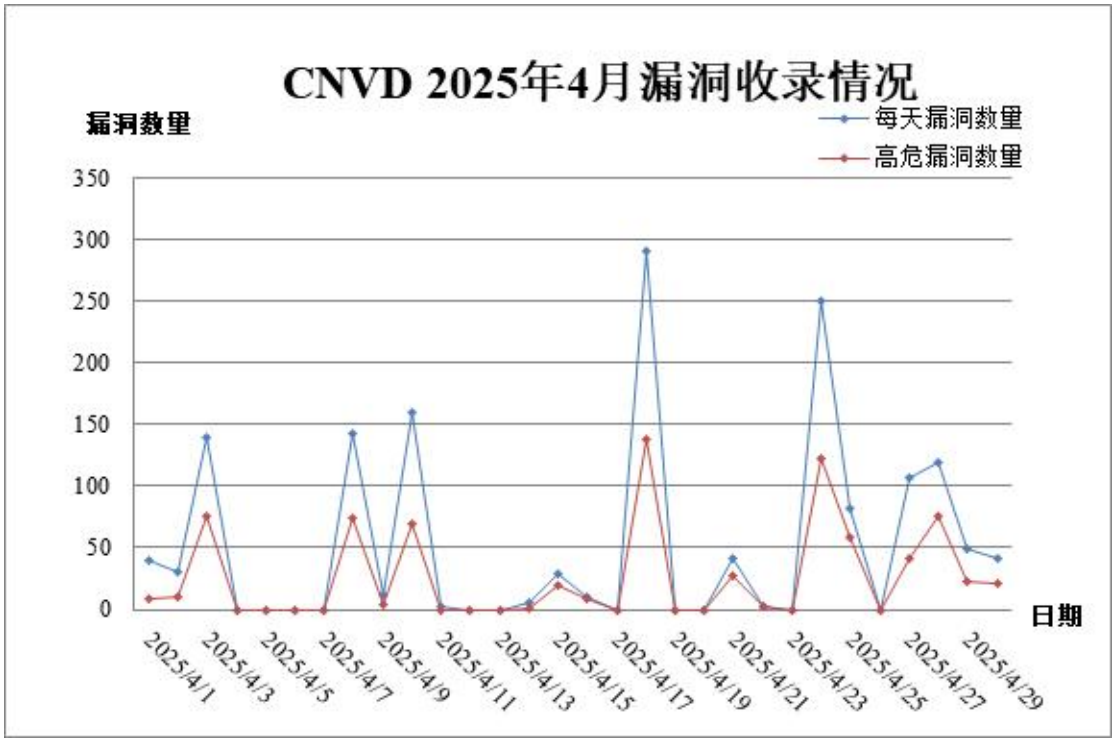
根据漏洞影响对象的类型，漏洞可分为 WEB 应用、应用程序、操作系统、网络设备（交换机、路由器等网络端设备）、数据库、安全产品（如防火墙、入侵检测系统等）、智能设备（物联网终端设备）和区块链漏洞。不同类型漏洞的分布如图 1 所示，本月 WEB 应用占比例较大。与前 12 个月相比，操作系统、WEB 应用和智能设备（物联网终端设备）漏洞的数量处于高位，应用程序、网络设备（交换机、路由器等网络端设备）、数据库和安全产品漏洞的数量处于低位。



漏洞类型分布

（二）漏洞趋势

4 月，CNVD 收集整理信息安全漏洞 1554 个，与前 12 个月平均收录数量 1415 个相比，处于高位；本月高危漏洞 780 个，与前 12 个月高危漏洞平均收录数量 689 个相比，处于高位。4 月的总体漏洞趋势如图所示



4 月份漏洞发布趋势

附录：4 月份重要漏洞信息汇总

4 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-2025-07780、CNVD-2025-07779 CNVD-2025-07782、CNVD-2025-07781 CNVD-2025-07785、CNVD-2025-07784 CNVD-2025-07783、CNVD-2025-07786 CNVD-2025-08885、CNVD-2025-08889	本月，Microsoft 多款产品存在安全漏洞。攻击者可利用漏洞绕过某些功能，提升权限，在目标主机上执行代码等。本月漏洞包括：Microsoft Windows Hello 安全功能绕过漏洞（CNVD-2025-07780）、Microsoft Windows DWM Core Library 权限提升漏洞（CNVD-2025-07779、CNVD-2025-07782、CNVD-2025-07781）、Microsoft Visual Studio 权限提升漏洞、Microsoft Windows Telephony Service 远程代码执行漏洞（CNVD-2025-07784、CNVD-2025-07783）、Microsoft Windows USB Print Driver 权限提升漏洞、Microsoft Windows Digital Media 权限提升漏洞（CNVD-2025-08885）、Microsoft Word 安全功能绕过漏洞（CNVD-2
		其他编号	CVE-2025-26635、CVE-2025-24073 CVE-2025-24058、CVE-2025-24074 CVE-2025-29802、CVE-2025-21221 CVE-2025-21222、CVE-2025-26639 CVE-2025-26640、CVE-2025-29816	
		发布时间	2025-04-18	
		影响产品	Microsoft Windows Server 2019 Microsoft Windows Server 2022 Microsoft Windows Server 2016 Microsoft Windows Server 2025 Microsoft Windows Server 2008 Microsoft Windows Server 2012 Microsoft Windows 10 21H2	

			Microsoft Windows 11 22H2 Microsoft Visual Studio 2022 Microsoft Office 2016 Microsoft Word 2016 Microsoft Office 2019 Microsoft 365 Apps for Enterprise Microsoft Office LTSC 2021 Microsoft Office LTSC for Mac 2021 Microsoft Office LTSC 2024 Microsoft Office LTSC for Mac 2024	025-08889）等。
2	Google 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-07516、CNVD-2025-07523 CNVD-2025-07522、CNVD-2025-07521 CNVD-2025-07520、CNVD-2025-07531 CNVD-2025-07530、CNVD-2025-07529 CNVD-2025-07534、CNVD-2025-07596	本月，Google 多款产品存在安全漏洞。攻击者可利用漏洞获取敏感信息，绕过 parcel 不匹配缓解措施并提升权限，执行远程代码等。本月漏洞包括：Google Chrome 输入验证错误漏洞（CNVD-2025-07516）、Google Android 缓冲区溢出漏洞（CNVD-2025-07523、CNVD-2025-07531、CNVD-2025-07529、CNVD-2025-07596）、Google Android 权限提升漏洞（CNVD-2025-07522、CNVD-2025-07520）、Google gVisor 权限提升漏洞（CNVD-2025-07534）、Google Android 信息泄露漏洞（CNVD-2025-07521、CNVD-2025-07530）等。
		其他编号	CVE-2025-3070、CVE-2024-43771 CVE-2024-49732、CVE-2024-49734 CVE-2024-49744、CVE-2024-49745 CVE-2024-49733、CVE-2024-49747 CVE-2025-2713、CVE-2024-49738	
		发布时间	2025-04-14	
		影响产品	Google Chrome Google Android Google gVisor	
3	Cisco 多款产品存在	CNVD 编号	CNVD-2025-06483、CNVD-2025-06645	本月，Cisco 多款产品存在安全漏

	安全漏洞		CNVD-2025-06671、CNVD-2025-06670 CNVD-2025-06672、CNVD-2025-06738 CNVD-2025-06741、CNVD-2025-06740 CNVD-2025-06739、CNVD-2025-06742	洞。攻击者可利用漏洞下载恶意文件，读取系统上的任意文件，将权限提升至 root。本月漏洞包括：Cisco Secure Web Appliance 输入验证错误漏洞、Cisco IOS XR 数据伪造问题漏洞、Cisco Application Policy Infrastructure Controller 跨站脚本漏洞、Cisco Identity Services Engine 路径遍历漏洞（CNVD-2025-06671、CNVD-2025-06672、CNVD-2025-06738）、Cisco Expressway Series 跨站请求伪造漏洞（CNVD-2025-06741、CNVD-2025-06740、CNVD-2025-06742）、Cisco Integrated Management Controller 命令注入漏洞等。
		其他编号	CVE-2025-20183、CVE-2025-20143 CVE-2024-20529、CVE-2025-20116 CVE-2024-20527、CVE-2024-20532 CVE-2024-20254、CVE-2024-20255 CVE-2024-20295、CVE-2024-20252	
		发布时间	2025-04-07	
		影响产品	Cisco Secure Web Appliance Cisco IOS XR Cisco Identity Services Engine Cisco Application Policy Infrastructure Controller (APIC) Cisco Expressway Series Cisco Integrated Management Controller	
4	Adobe 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-06309、CNVD-2025-06310 CNVD-2025-07241、CNVD-2025-07243 CNVD-2025-07244、CNVD-2025-07245 CNVD-2025-07246、CNVD-2025-07248 CNVD-2025-07250、CNVD-2025-07251	本月，Adobe 多款产品存在安全漏洞。攻击者可利用漏洞读取任意文件系统，绕过安全功能，在当前用户的上下文中执行任意代码。本月漏洞包括：Adobe Illustrators 栈缓冲区

		其他编号	CVE-2025-21163、CVE-2024-49530 CVE-2025-30297、CVE-2025-30295 CVE-2025-30304、CVE-2025-27200 CVE-2025-27199、CVE-2025-30290 CVE-2025-30282、CVE-2025-30281	溢出漏洞（CNVD-2025-06309）、Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2025-06310）、Adobe Animate 内存错误引用漏洞（CNVD-2025-07245）、Adobe Animate 堆缓冲区溢出漏洞（CNVD-2025-07246）、Adobe ColdFusion 路径遍历漏洞（CNVD-2025-07248）、Adobe ColdFusion 身份验证不当漏洞、Adobe ColdFusion 访问控制不漏洞、Adobe FrameMaker 堆缓冲区溢出漏洞（CNVD-2025-07243）、Adobe FrameMaker 越界写入漏洞（CNVD-2025-07241、CNVD-2025-07244）等。
		发布时间	2025-04-15	
		影响产品	Adobe Illustrators Adobe Acrobat reader Adobe Framemaker Adobe Animate 2024 Adobe ColdFusion 2025 Adobe ColdFusion 2023 Adobe ColdFusion 2021	
5	DELL 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-06613、CNVD-2025-06614 CNVD-2025-06615、CNVD-2025-06616 CNVD-2025-06617、CNVD-2025-06618 CNVD-2025-06619、CNVD-2025-06620 CNVD-2025-06621、CNVD-2025-06622	本月，DELL 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操作系统命令。本月漏洞包括：Dell Unity OS 命令注入漏洞（CNVD-2025-06613、CNVD-2025-06614、CNVD-2025-06615、CNVD-2025-06616、CNVD-2025-06617、CNVD-2025-06618、CNVD-2025-06619、CNVD-2025-06620、CNVD-2025-06621、C
		其他编号	CVE-2024-49565、CVE-2024-49564 CVE-2025-24378、CVE-2024-49563 CVE-2025-24382、CVE-2025-24386 CVE-2025-24385、CVE-2025-243	

			77 CVE-2025-24380、CVE-2025-24379	NVD-2025-06622）等。
		发布时间	2025-04-07	
		影响产品	Dell Unity	
6	Siemens 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-08350、CNVD-2025-08351 CNVD-2025-08352、CNVD-2025-08353 CNVD-2025-08354、CNVD-2025-08355 CNVD-2025-08357、CNVD-2025-08356 CNVD-2025-08358、CNVD-2025-08360	本月，Siemens 多款产品存在安全漏洞。攻击者可利用漏洞导致绕过授权控制和执行任意代码等。本月漏洞包括：Siemens TeleControl Server Basic SQL 注入漏洞（CNVD-2025-08350、CNVD-2025-08351、CNVD-2025-08352、CNVD-2025-08353、CNVD-2025-08354、CNVD-2025-08355、CNVD-2025-08357、CNVD-2025-08356、CNVD-2025-08358、CNVD-2025-08360）等。
		其他编号	CVE-2025-31351、CVE-2025-31349 CVE-2025-31343、CVE-2025-30032 CVE-2025-30031、CVE-2025-30003 CVE-2025-29905、CVE-2025-30030 CVE-2025-30002、CVE-2025-32827	
		发布时间	2025-04-24	
		影响产品	Siemens TeleControl Server Basic	
7	Xiaomi 多	CNVD 编	CNVD-2025-06293、CNVD-2025-0	本月，Xiaomi 多款

	款产品存在安全漏洞	号	6296 CNVD-2025-06295、CNVD-2025-06294 CNVD-2025-06298、CNVD-2025-06297 CNVD-2025-06300、CNVD-2025-06299 CNVD-2025-06303、CNVD-2025-06302	产品存在安全漏洞。攻击者可利用漏洞获取敏感信息，执行任意代码或导致拒绝服务，通过劫持 ISP 或上层路由器来获取权限等。本月漏洞包括：Xiaomi GetApps 代码执行漏洞、Xiaomi Router 命令注入漏洞（CNVD-2025-06296、CNVD-2025-06295、CNVD-2025-06298）、Xiaomi Router 缓冲区溢出漏洞（CNVD-2025-06294）、Xiaomi cloud service Application 跨站脚本漏洞、Xiaomi Mi Sound 信息泄露漏洞、Xiaomi SmartHome APP 信息泄露漏洞、Xiaomi Millet mobile phones 文件上传漏洞、Xiaomi AX1800 等命令注入漏洞等。
		其他编号	CVE-2023-26322、CVE-2023-26320 CVE-2023-26319、CVE-2023-26318 CVE-2023-26317、CVE-2023-26316 CVE-2020-14126、CVE-2020-14114 CVE-2019-15843、CVE-2020-14102	
		发布时间	2025-04-02	
		影响产品	Xiaomi GetApps Xiaomi router Xiaomi cloud service Application Xiaomi Mi Sound Xiaomi SmartHome Xiaomi Millet mobile phones Xiaomi AX1800 rom Xiaomi RM1800 root	
8	Apple 多款产品存在安全漏洞	CNVD 编号	CNVD-2025-08895、CNVD-2025-08894 CNVD-2025-08900、CNVD-2025-08899 CNVD-2025-08898、CNVD-2025-08897 CNVD-2025-08902、CNVD-2025-08901 CNVD-2025-08904、CNVD-2025-08903	本月，Apple 多款产品存在安全漏洞。攻击者可利用漏洞访问私人信息，运行可执行代码，获取 root 权限等。本月漏洞包括：Apple iPadOS 权限问题漏洞（CNVD-2025-08895、CNVD-2025-08894、CNVD-2025-08899）、Apple macOS 访问控制漏洞（CNVD-2

				025-08900、CNVD-2025-08904）、Apple macOS 缓冲区溢出漏洞（CNVD-2025-08898、CNVD-2025-08897、CNVD-2025-08901）、Apple macOS 内存损坏漏洞（CNVD-2025-08902）、Apple macOS 权限提升漏洞（CNVD-2025-08903）等。