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 6 月上）

深信服科技股份有限公司

2025 年 6 月 16 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 6 月份（6.1-6.15）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，其中部分资讯内容由 AI 生成。

本期可以关注 DataEase H2 数据库远程代码执行漏洞(CVE-2025-49002)、Apache Kafka Connect 任意文件读取漏洞(CVE-2025-27817)，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：

国内政策热点：

1、李强签署国务院令 公布《政务数据共享条例》

2、2025 上海“磐石行动”：AI+网络安全成新赛道 行业年复合增长 9.2%

3、广东省网络数据安全与个人信息保护协会成立

国际政策热点：

1、美英联合发布《AI 数据安全：用于训练和操作 AI 系统的数据安全最佳实践》

2、微软推出面向政府的免费欧盟网络安全计划

3、英国持续强化网络战能力

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）国内政策热点

1、李强签署国务院令 公布《政务数据共享条例》

据新华社北京 6 月 3 日发文，国务院总理李强日前签署国务院令，公布《政务数据共享条例》（以下简称《条例》），自 2025 年 8 月 1 日起施行。《条例》旨在推进政务数据安全有序高效共享利用，提升政府数字化治理能力和政务服务效能，全面建设数字政府。

《条例》第五条是强化保障措施。按照谁管理谁负责、谁使用谁负责的原则，明确各环节安全责任主体，强调需求部门在使用依法共享政务数据过程中的安全管理责任。细化政府部门和受托方政务数据安全保护义务，明确个人信息保护及处理投诉举报要求。提出政务数据共享经费保障和预算管理要求。

原文链接：

李强签署国务院令 公布《政务数据共享条例》_中国政府网

2、2025 上海“磐石行动”：AI+网络安全成新赛道 行业年复合增长 9.2%

近日，上海举办了 2025 年度“磐石行动”。上海以每年一度的“磐石行动”为抓手，持续织密网络安全、数据安全防护网。本届“磐石行动”50 支顶尖攻击队伍和 177 支防守队伍开展了长达 10 天的激烈鏖战。

上海市通信管理局局长王天广表示，本届“磐石行动”形成三方面显著成效：一是实战成果彰显防御新高度。各参演单位在高强度攻防中实现防御能力突破，动态防御机制在实战中得到充分检验，网络安全风险预警与应急响应的协同联动效能显著增强。二是暴露问题并检视深层隐患。推动企业从技术架构、管理机制、人员意识三个层面深入查摆问题，为构建“能打仗，打胜仗”的防护体系提供了改进方向。三是创新实践筑牢安全韧性根基。面对人工智能快速发展带来的新型安全挑战，本届演练创新设置“AI 安全”等专项场景，在人工智能安全开发、

合规运营、风险防控等领域形成标准化防护能力，为构建安全可信的人工智能产业生态筑牢网络安全屏障。

原文链接：

实探“磐石行动”：AI+网络安全成新赛道 行业年复合增长 9.2%|上海证券报

3、广东省网络数据安全与个人信息保护协会成立

6 月 12 日，广东省网络数据安全与个人信息保护协会正式成立，该协会是我国首个网络数据安全领域的社会组织，也是我国首个个人信息权益保护领域的社会组织。协会将推动制定新兴行业或领域的个人信息保护团体标准，形成具有示范效应的“广东实践”。

广东省网络数据安全与个人信息保护协会的成立，对于搭建务实平台，协助构建多元协同、高效运行的治理机制，防范网络数据安全风险，加强个人信息保护，包括深化合规引导，以及立足广东实际，牵头研制具有示范性的个人信息保护团体标准，助力行业规范，都意味着一个社会参与、共治共享的新阶段。

原文链接：

守护全民数据安全，广东激活社会共治_南方+_南方 plus

（二）国际政策热点

1、美英联合发布《AI 数据安全：用于训练和操作 AI 系统的数据安全最佳实践》

近期，美国国家安全局（NSA）人工智能安全中心（AISC）发布了一份联合网络安全信息简报（CSI），题为《AI 数据安全：用于训练和操作 AI 系统的数据安全最佳实践》。该简报旨在为 AI 系统的数据安全提供最佳实践和建议，强调在 AI 系统的开发、测试和运行过程中，保护数据对于确保 AI 系统的准确性、可靠性和完整性至关重要。

该最佳实践适用于他国国防部、国家安全系统和国防工业基础等组织，尤其是那些已经在日常运营中使用 AI 系统或计划将 AI 集成到其基础设施中的机构。NSA 鼓励这些组织将简报中的最佳实践和缓解策略应用于其任务环境，以加强 AI

系统的安全性并保护敏感和关键数据。

原文链接：

美英联合发布《AI 数据安全：用于训练和操作 AI 系统的数据安全最佳实践》

2、微软推出面向政府的免费欧盟网络安全计划

6 月 4 日，微软宣布了一项新的“欧洲安全计划”，承诺加强欧洲各国政府的网络安全，旨在防御俄罗斯、伊朗和朝鲜等国家支持的行为者的攻击。该计划对所有欧盟国家免费，覆盖欧盟 27 国及候选国、欧洲自由贸易联盟成员国、英国、摩纳哥及梵蒂冈。微软数字犯罪部门和威胁分析中心将提供情报渠道，根据各国需求定制 AI 驱动威胁洞察，提供实时漏洞预警和补救指导，并跟踪深度伪造威胁。此外，微软还将与欧洲刑警组织、互联网服务提供商协作，加强用户端防护。

原文链接：

微软宣布启动新的安全计划，免费提升欧洲各国政府的网络安全水平 - IT 之家

3、英国持续强化网络战能力

据 6 月 10 日报道，英国国防部近期宣布，将斥资 10 亿英镑(约合 13.5 亿美元)建设“数字目标定位网络”。为此，英国将组建新的网络与电磁司令部，并招募相关人员，全面强化英军网络战能力，使网络和电磁行动与其他军事行动紧密联动。

为配合“数字目标定位网络”计划，英国将成立一个新的网络与电磁司令部。新司令部将抽调陆海空三军人员共同组建，负责领导网络防御行动，并与国家网络部队协调运用网络进攻力量。对英国来说，网络攻击并非全新领域。过去 5 年，英国政府通信总部和国防部共同组建的国家网络部队，一直在开展网络攻击行动。

原文链接：

英持续强化网络战能力 - 国际军事 - 华夏经纬网

二、安全热点时事资讯

（一）国内安全事件

1、西宁一单位关键业务信息系统遭受网络攻击致业务系统瘫痪

时间：6 月 2 日

概况：

西宁市某单位关键业务信息系统遭受网络攻击，单位内 26 台服务器感染勒索病毒，并对大量文件进行加密锁定，导致该单位关键业务信息系统瘫痪，部分业务无法正常开展。期间，攻击者疑似诱骗该单位支付一定数量的 Bit 币（网络虚拟货币）后，恢复相关业务数据。通过现场民警的初步勘查后发现，攻击者在 5 月 31 日至 6 月 2 日针对该单位关键业务信息系统开展持续性的网络攻击，期间，部分业务系统的安全防护设备多次预警，该单位相关负责人及运维人员均未引起重视，并未采取相关应急措施，导致相关服务器被感染。截至发文时，该单位已停止相关业务，感染主机已采取断网隔离处理，相关业务系统正在紧急恢复当中。

安全防御措施：

西宁网警梳理了 12 条如何防范勒索病毒的安全措施，再次提醒关键信息系统运营单位做好网络安全防护，避免信息系统被感染，导致业务无法正常运行：

1、摸清本单位网络资产底数，对已停止业务的老旧系统采取断网断电等措施。

2、定期对本单位的业务系统及网络设备开展漏洞、弱口令等安全隐患的排查，并及时整改。

3、关闭高危端口，加强网络边界防御，安装边界安全防御设备，并配置防护策略。

4、及时更新服务器、主机、操作系统、软件的安全补丁，提高系统安全性。

5、选择可靠的杀毒软件，并定期更新病毒库，有效检测和清除勒索病毒。

6、不要随意打开未知邮件和链接，并禁止邮件和连接附件自动下载运行。

7、定期备份数据，重要数据需采取异地备份，避免备份文件被加密或损坏。

8、定期对系统日志进行分析研究及时发现系统中的可疑 IP 以及相关隐患，提高安全策略并加强对可疑的 IP 进行屏蔽等。

9、在非必要时，禁止利用公共网络远程连接单位内部网络及关键信息系统。

10、严格限制系统访问权限，避免过度权限导致的安全风险。

11、禁止内外网“U”盘等存储介质的交叉使用。传输、存储等可使用具备安全防御功能的介质。

12、如遇到勒索病毒攻击，及时排查服务器、主机等被感染的网络设备，并断网隔离。

原文链接：

西宁一单位关键业务信息系统遭受网络攻击

2、北京网信办通报两家企业因未授权访问漏洞导致数据窃取被罚款

时间：6 月 13 日

概况：

据网信北京发文，今年以来，北京市网信办持续加强数据安全领域执法力度。近期，部分企业因未依法履行数据安全保护义务，其相关系统、服务器或数据库存在未授权访问漏洞和弱口令漏洞问题，造成数据被窃取，北京市网信办依法对涉案企业进行了查处。针对违法情况，北京市网信办依据《中华人民共和国数据安全法》第四十五条，对北京某科技公司、北京某有限公司作出警告，并分别处五万元罚款的行政处罚。

官方安全警示及建议：

北京市网信办相关负责人表示，数据安全关乎人民群众切身利益，关乎国家安全和社会稳定。部分企业因业务需求，需要收集储存大量个人信息等敏感数据，一

旦被窃取或非法利用，会造成社会危害。企业应当依法履行数据安全保护义务，建立健全全流程数据安全管理制度，落实网络安全等级保护要求，加强数据访问权限管控和端口管理力度，设置符合强度要求的登录密码，配置访问 IP 白名单，通过技术手段对个人信息数据进行脱敏、加密处理，定期组织开展安全培训、漏洞扫描等相关工作。下一步，北京市网信办将针对数据安全保护义务履行不力，造成重要数据遭窃取的违法违规行为加强监督执法，营造安全稳定的网络环境。

原文链接：

北京市网信办加强数据安全领域执法工作 依法查处两家违法企业

（二）国际安全事件

1、德国大众汽车集团遭勒索攻击，车主账户数据、核心身份验证令牌等敏感数据泄露

时间：6 月 1 日

概况：

据媒体报道，德国汽车巨头大众汽车集团正面临新一轮严峻的数据泄露危机。全球知名勒索软件团伙 Stormous 近日高调宣称，入侵了大众系统并窃取核心数据，将这家全球销量第二大、营收第一的汽车制造商列入其暗网泄密网站。OAuth、JWT 等高级身份令牌一旦失窃，攻击者可能获得远超传统数据泄露的破坏力，甚至威胁车辆控制安全。车辆位置信息的暴露，更是将用户隐私置于危险的境地。

此次勒索攻击事件也再次为整个汽车行业敲响了警钟，在竞相开发更智能的汽车时，数据安全与用户隐私保护必须成为同等重要的核心考量，而非事后补救的附属品。

安全防范建议：（针对汽车制造等行业）

1）强化身份与访问管理（IAM）

令牌动态管理：对 OAuth、JWT 等令牌实施短有效期（≤1 小时）和自动轮换机制，吊销未使用令牌。

特权账号保护：对管理员账户启用硬件密钥认证，操作需双人复核。

2）加强车联网安全专项防护

车辆 API 隔离：将车辆控制 API 与用户服务 API 部署在不同网络域，实施物理隔离防火墙。

安全启动与固件签名：确保车载系统固件通过加密签名验证，防止未授权代码执行。

3）加强供应链安全管控

第三方安全评估：对所有供应商（尤其是软件组件提供商）进行年度安全审计，要求符合标准。

漏洞赏金计划：设立专项奖金鼓励白帽黑客报告车联网系统漏洞（如车辆远程控制漏洞）。

原文链接：

德国大众汽车集团遭勒索攻击，车主账户数据、核心身份验证令牌等敏感数据泄露

2、美国财产和意外保险公司 Erie Insurance 证实遭遇网络攻击，导致业务中断

时间：6 月 7 日

概况：

Erie Insurance 及其管理公司 Erie Indemnity Company 确认，近日的业务中断和网站平台故障，源于上周末遭遇的一起网络攻击事件。

Erie Indemnity Company 是 Erie Insurance Group 的管理机构，该集团是一家美国的财产和意外保险公司，现有超过 600 万份有效保单，提供汽车、住房、寿险和商业保险等服务，主要通过独立代理商运营。从 2025 年 6 月 7 日（周六）起，Erie Insurance 的网站和业务系统陆续出现大范围故障，客户无法登录门户网站，部分人报告称无法提交理赔申请或接收相关文件。Erie Indemnity Company 向美国证券交易委员会（SEC）提交了 8-K 文件，披露公司于 6 月 7 日发现“异常的网络活动”。

安全防范建议：（针对金融保险等行业）

1）构建韧性基础设施

网络分段隔离：将核心业务系统（如理赔、支付）与办公网络隔离，部署微隔离技术。

离线备份策略：每日全量备份至离线介质，每周验证备份可恢复性，确保备份与生产环境隔离。

2）提升威胁检测能力

EDR+XDR 联动：部署端点检测（EDR）结合全流量分析，对横向移动、异常加密流量实时拦截。

威胁情报整合：订阅行业威胁情报，自动阻断已知勒索软件 IP 和 C2 域名。

3）应急响应与灾难恢复措施

自动化故障转移：核心系统配置双活架构。

勒索软件专项预案：明确断网隔离流程、取证数据保留要求、是否支付赎金的决策机制（建议拒绝支付）。

原文链接：

【安全圈】Erie Insurance 证实遭遇网络攻击，导致业务中断

3、黑客团伙伪装 IT 支持实施语音钓鱼，瞄准欧美零售、酒店及教育行业

时间：6 月 9 日

概况：

一个自称“The Community”（简称 Com）的青少年黑客组织正通过语音钓鱼（vishing）和恶意软件组合攻击，针对欧美酒店、零售及教育行业的云服务展开数据窃取。该活动被谷歌追踪为 UNC6040，已影响约 20 家机构。

据谷歌威胁情报组（GTIG）最新报告披露，该组织冒充公司内部技术人员，通过电话实施社会工程攻击，主要针对跨国公司中讲英语的员工，诱骗其授权访问敏感系统，尤其是广泛使用的客户关系管理（CRM）平台——Salesforce。尽管 Salesforce 是其主要目标，但 UNC6040 的野心并不限于此。一旦获得初始凭证，

该组织还会在企业内部横向移动，进一步渗透 Okta、Microsoft 365 等平台。这些更广泛的访问权限使其能够收集更多有价值的数据，进一步巩固控制力，为日后实施更严重的勒索行动铺路。

安全防范建议：

谷歌 GTIG 建议企业采取以下措施以降低此类安全事件发生的风险：

严格权限管理：限制 Data Loader 等强大工具的使用权限，仅允许真正有需要的员工使用，并定期审核其权限。

控制连接应用：管理可以接入 Salesforce 的连接应用，所有新应用应通过正式审批流程。

限制 IP 范围：为了防止攻击者通过 VPN 访问系统，应将登录和应用授权限制在可信 IP 地址范围内。

实时监控：使用如 Salesforce Shield 等安全平台，可实时监测和阻止大规模数据导出行为。

强化多因子认证（MFA）：虽然 MFA 并非万能，但它仍然是防范帐户被盗的有效手段，特别是在用户受过识别钓鱼电话等社交工程攻击的训练时。

原文链接：

【安全圈】黑客冒充 IT 技术支持打电话渗透企业系统，谷歌披露攻击细节

三、安全风险通告

（一） DataEase H2 数据库远程代码执行漏洞(CVE-2025-49002)

漏洞名称:DataEase H2 数据库远程代码执行漏洞(CVE-2025-49002)

漏洞描述：2025 年 6 月 5 日，深瞳漏洞实验室监测到一则 DataEase 组件存在代码执行漏洞的信息。DataEase 存在一个远程代码执行漏洞，**未授权攻击者可以利用 CVE-2025-49001 绕过 JWT 认证，通过 JDBC 远程加载恶意内容，执行任意代码导致服务器失陷**。

漏洞编号：CVE-2025-49002，漏洞威胁等级：高危。

组件介绍：

DataEase 是一种关系型数据库管理系统（RDBMS），它最初于 1981 年由 DataEase International 公司开发。它是一种易于使用的数据库软件，旨在为非专业人士提供一种简单的方法来创建和管理数据库。DataEase 具有图形用户界面和可视化工具，使用户可以轻松地创建表格、查询、报告和表单。它还具有内置的安全性和数据完整性功能，以确保数据的安全和准确性。

影响范围：

目前受影响的 DataEase 版本：

DataEase ≤ 2.10.8

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>：严重，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 DataEase 更新到 v2.10.10 及以上版本。

下载链接：

https://github.com/dataease/dataease/releases/tag/v2.10.10

深信服解决方案：

1、风险资产发现

支持对 DataEase 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:0017588。

【深信服漏洞评估工具 TSS】已发布资产检测方案，指纹 ID:0017588。

2、漏洞主动检测

支持对 DataEase H2 数据库远程代码执行漏洞(CVE-2025-49002)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-2025-00479。

【深信服漏洞评估工具 TSS】已发布检测方案，规则 ID:SF-2025-00986。

【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-2025-00986。

【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-2025-00479。

3、漏洞安全监测

支持对 DataEase H2 数据库远程代码执行漏洞(CVE-2025-49002)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:11029253。

【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:11029253。

【深信服安全检测与响应平台 XDR】已发布监测方案，规则 ID:11029253。漏洞安全防护支持对 DataEase H2 数据库远程代码执行漏洞(CVE-2025-49002)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:11029253。

【深信服 Web 应用防火墙 WAF】已发布防护方案，规则 ID:11029253。

【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:11029253。

【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:11029253。

（二） Apache Kafka Connect 任意文件读取漏洞(CVE-2025-27817)

漏洞名称 ：Apache Kafka Connect 任意文件读取漏洞(CVE-2025-27817)

漏洞描述：2025 年 6 月 10 日，深瞳漏洞实验室监测到一则 Apache-Kafka 组件存在任意文件读取漏洞的信息。Apache Kafka Connect 组件存在任意文件读取漏洞，**未授权的攻击者可以利用该漏洞读取任意文件，导致敏感信息泄露。**

漏洞编号：CVE-2025-27817，漏洞威胁等级：**高危**。

组件介绍：

Apache Kafka 是一个开源分布式事件流平台，被数千家公司用于高性能数据管道、流分析、数据集成和任务关键型应用程序。

影响范围：

目前受影响的 Apache-Kafka 版本：

3.1.0 ≤ Apache Kafka < 3.9.1

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，无需授权即可读取任意文件。

<综合评定威胁等级>：高危，能导致敏感信息泄露。

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 Apache Kafka 更新到 3.9.1 及以上版本。

链接如下：

https://github.com/apache/kafka/tags

深信服解决方案：

风险资产发现

支持对 Apache-Kafka 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：

【深信服统一端点安全管理系统 aES】已发布资产检测方案，指纹 ID:0006168。

【深信服云镜 YJ】已发布资产检测方案，指纹 ID:0006168。

【深信服漏洞评估工具 TSS】已发布资产检测方案，指纹 ID:0006168。

四、微软安全通告

（一） 漏洞概要

2025 年 6 月 11 日（北京时间），微软发布了 2025 年 6 月安全更新，共发布了 69 个 CVE 的补丁程序，同比上月减少了 13 个。

在漏洞安全等级方面，存在 10 个标记等级为“Critical”的漏洞，58 个漏洞被标记为“Important/High”等级的漏洞； 在漏洞类型方面，主要有 27 个远程代码执行漏洞，14 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 69 个，有 10 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

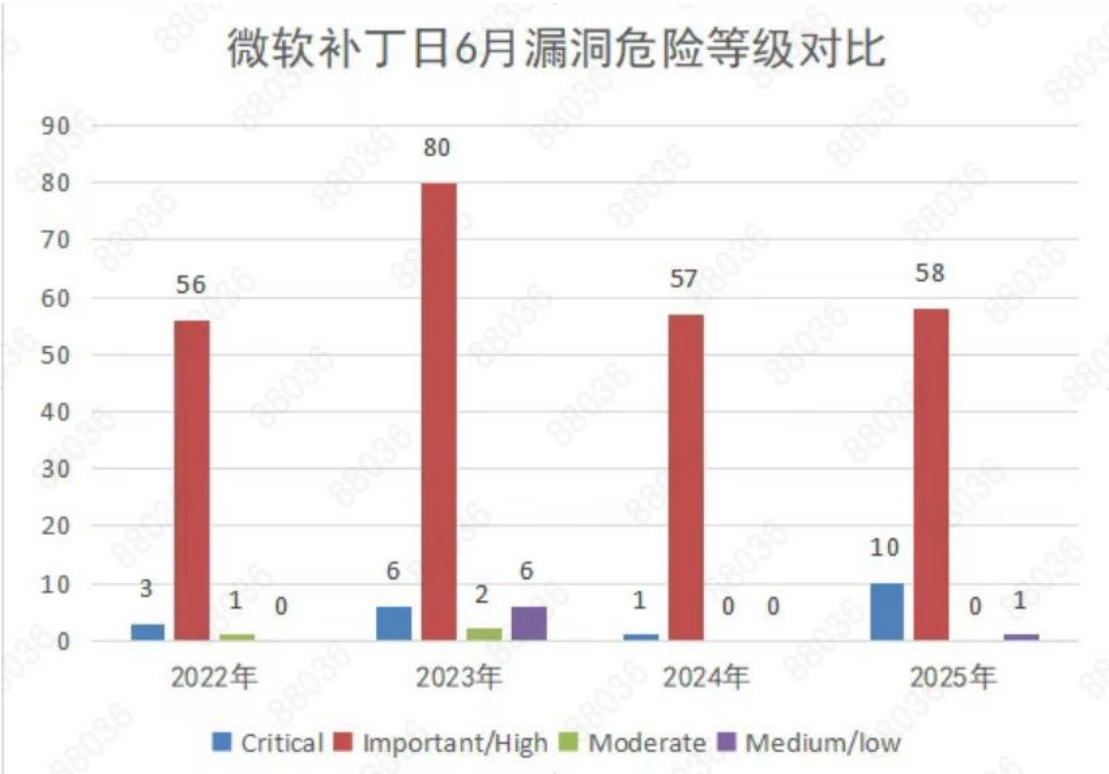
特殊情况，初步估计微软在今年七月份公布的漏洞数将比今年六月份少。漏洞数量将会维持在 80 个左右。

2 、历史微软补丁日 6 月漏洞对比

2022—2025 年，6 月份的 Windows 补丁趋势如下图：

历年 6 月份微软 Windows 补丁趋势

2022-2025 年，6 月份的漏洞危险等级趋势和数量如下图：



历年 6 月份微软漏洞危险等级对比

2022-2025 年，6 月份的漏洞各个类型数量对比如下图：

微软近年 6 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 6 月份爆发的漏洞相较于去年增多。本月出现了 69 个漏洞补丁，并且有 10 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 10 个“Critical”等级的漏洞，相较去年增加了 900%；本月出现了 58 个“Important/High”等级的漏洞，相较去年增加了约 2%。

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 类型的漏洞数量减少，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

Web 分布式创作和版本控制（WEBDAV）远程代码执行漏洞 CVE-2025-33053

WebDAV（Web 分布式创作和版本控制）是对 HTTP 协议的扩展，允许客户端直接在远程 Web 服务器上创建、编辑、移动、复制和删除文件。WebDAV 可通过端口 80 / 443 使用，广泛内建于操作系统和 Web 服务器中

其中存在远程代码执行漏洞，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。

Windows Netlogon 特权提升漏洞 CVE-2025-33070

Windows 的 Netlogon 服务用于在域成员与域控制器之间建立和维护安全通道，实现 NTLM 或 Kerberos 的传递式身份验证；它还负责域控制器定位与机器账户的认证。

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，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 KDC 代理服务（KPSSVC）远程代码执行漏洞 CVE-2025-33071

Windows 的 KDC 代理服务(KPSSVC) 是一个在边缘/远程访问服务器(如 RD Gateway、DirectAccess)上运行的 HTTPS 中继服务，监听 /KdcProxy 接口(通常 443 端口)，用于将 Kerberos 请求(包括凭证获取和密码更改)通过 TLS 代理传输到内部域控制器，无需直连 KDC，可支持远程设备认证与密码修改。

其中存在远程代码执行漏洞，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
Web 分布式创作和版本控制 (WEBDAV) 远程代码执行漏洞 CVE-2025-33053	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 Coreinstallation) 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
Windows Netlogon 特权提升漏洞 CVE-2025-33070	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 Coreinstallation) 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
Windows KDC 代理服务 (KPSSVC) 远程代码执行漏洞 CVE-2025-33071	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

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-2025-33053

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33070

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33071