奇安信
威胁情报中心

2025年中
网络安全漏洞
威胁态势研究报告

2025年7月

前言 Preface

随着数字化进程的加速与新兴技术的普及，网络安全形势日益严峻。漏洞作为网络攻击的关键切入点，其数量、类型及影响范围的变化对网络安全态势有着决定性影响。本报告基于奇安信 CERT 公众号上半年数据，对 2025 年中漏洞态势进行深入研究，旨在为企业和相关机构提供全面、准确的漏洞信息，助力其制定有效的安全防护策略。

摘要 summary

2025上半年漏洞态势的关键发现：

漏洞数量持续攀升：2025年中新增漏洞23351个，其中高危漏洞占比43.5%，高危漏洞占比扩大且利用窗口期急剧缩短。

漏洞利用速度的指数级提升使传统“修补窗口期”大幅压缩：2025年漏洞利用呈现明显的加速化趋势，攻击者从漏洞披露到武器化部署的周期缩短至历史新低。利用漏洞作为初始攻击手段的案例同比增长34%，占所有入侵事件的20%。漏洞利用已连续五年蝉联最常见的初始感染媒介（占比33%），超越钓鱼攻击成为企业面临的首要威胁。

利用模式产业化升级：漏洞利用的产业化特征在2025年尤为突出，攻击者采用战前储备与战时挖掘双轨并行策略。一方面，APT组织加大0day漏洞的战略储备，另一方面，攻击者利用自动化工具实现漏洞挖掘、武器化、分发利用的全链条协作，形成“漏洞利用即服务”（Exploitation-as-a-Service）的商业模式。

复合攻击链成主流：攻击者更倾向于构建多阶段、多技术的复合攻击链，漏洞利用只是其中一环。攻击往往始于单点漏洞，但通过横向移动、权限提升和持久化控制形成深度渗透。

国产软件漏洞呈上升趋势：218个国产软件漏洞被披露，OA系统和网络设备成为攻击重点目标，暴露了国内软件在安全设计阶段的不足。

2025下半年漏洞发展趋势展望：

AI驱动的漏洞挖掘：攻击者利用大模型分析开源代码，漏洞发现效率提升3-5倍。同时，对抗性机器学习被用于生成绕过检测的漏洞利用代码。

量子计算威胁显现：随着量子计算机发展，传统公钥加密算法面临破解风险，抗量子密码迁移需求迫切。

云原生漏洞架构缺陷引爆风险：Kubernetes配置错误、服务网格漏洞和Serverless函数注入将导致容器逃逸事件增长50%。

物联网僵尸网络升级：利用TOTOLink、D-Link等设备漏洞组建的僵尸网络规模可达百万级，DDoS攻击峰值突破5Tbps。

软件供应链攻击常态化：开源库和第三方组件漏洞占比将超60%，类似XZUtils后门事件的影响范围和隐蔽性进一步提升。

目录 Table of contents

第一章 2025年中漏洞态势分析

一、漏洞数量统计与趋势

二、漏洞类型分布与威胁分析

三、漏洞影响厂商与行业分布

四、关键漏洞占比情况

五、漏洞标签占比情况

六、漏洞热度排名TOP 10

七、2025年中最危险的CWE类型

八、漏洞修复时效性

第二章 重大漏洞案例分析

一、Apache Tomcat 管理面板遭受黑客组织定向暴力攻击

二、黑客利用 Windows WebDav 零日漏洞投放恶意软件

三、2025年第一个 Chrome 零日漏洞在间谍活动中被利用

四、披露闹剧给 CrushFTP 漏洞利用蒙上阴影

五、知名前端工具vite接连曝出4个任意文件读取漏洞

六、严重“IngressNightmare”漏洞危及 Kubernetes 环境

目录 Table of contents

第三章 关键种类漏洞分析

一、0day漏洞

二、在野利用相关漏洞

三、APT及勒索软件漏洞

四、国产软件相关漏洞

五、其它类别关键漏洞

第四章 2025年下半年漏洞新兴技术发展趋势展望

一、AI驱动的漏洞挖掘与利用：攻防智能化升级

二、量子计算冲击传统密码：迁移迫在眉睫

三、云原生与虚拟化漏洞：架构缺陷引爆风险

四、物联网设备漏洞：僵尸网络驱动大规模攻击

五、漏洞利用产业化：暗网经济助推攻击规模化

六、新兴威胁：供应链与AI泄露风险

第五章 漏洞处置建议

第六章 总结

第七章 奇安信漏洞情报服务订阅

01

第一章

2025年中漏洞态势分析

一、漏洞数量统计与趋势

2025年上半年，网络安全漏洞呈现出**数量持续攀升、高危漏洞占比扩大和利用窗口期急剧缩短**的三重特征。根据奇安信安全监测与响应中心（又称奇安信CERT）监测数据，新增漏洞23351个，总高危、极危漏洞数量为10154个，占总量的43.5%。仅6月第二周（6月9日-15日）就收录漏洞464个，其中高危漏洞222个（占比47.8%）。**这些数字反映出当前网络空间面临的系统性安全风险正在深化，威胁态势依然严峻。**

根据奇安信CERT的基于多维度的筛选流程,对其中5498个高潜在威胁漏洞进行了人工研判。奇安信CERT认为本年度值得重点关注的漏洞共683个[1]，达到发布安全风险通告标准的漏洞共179个[2]，并对其中21个漏洞进行深度分析[3]。

23351个
奇安信安全监测与响应中心共监测到新增漏洞

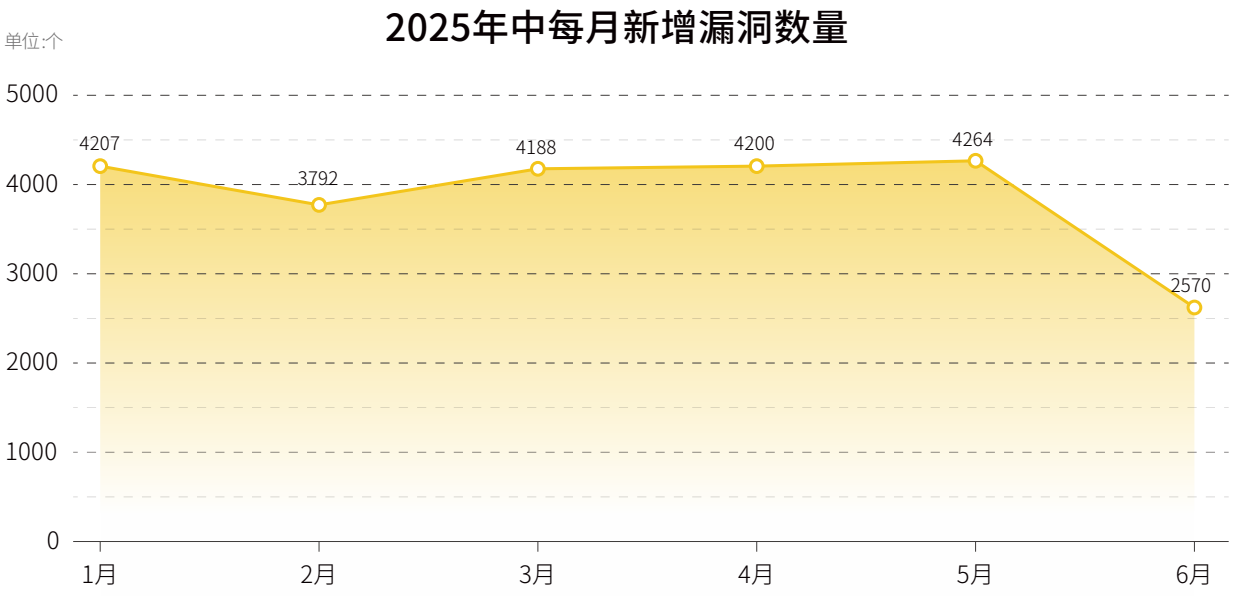
43.5%
占总量的

5498个
高危漏洞触发了人工研判

683个
本年度值得重点关注的漏洞

179个
达到奇安信CERT发布安全风险通告标准的漏洞

21个
漏洞进行深度分析



△图1-1 2024年奇安信CERT漏洞库每月新增漏洞信息数量

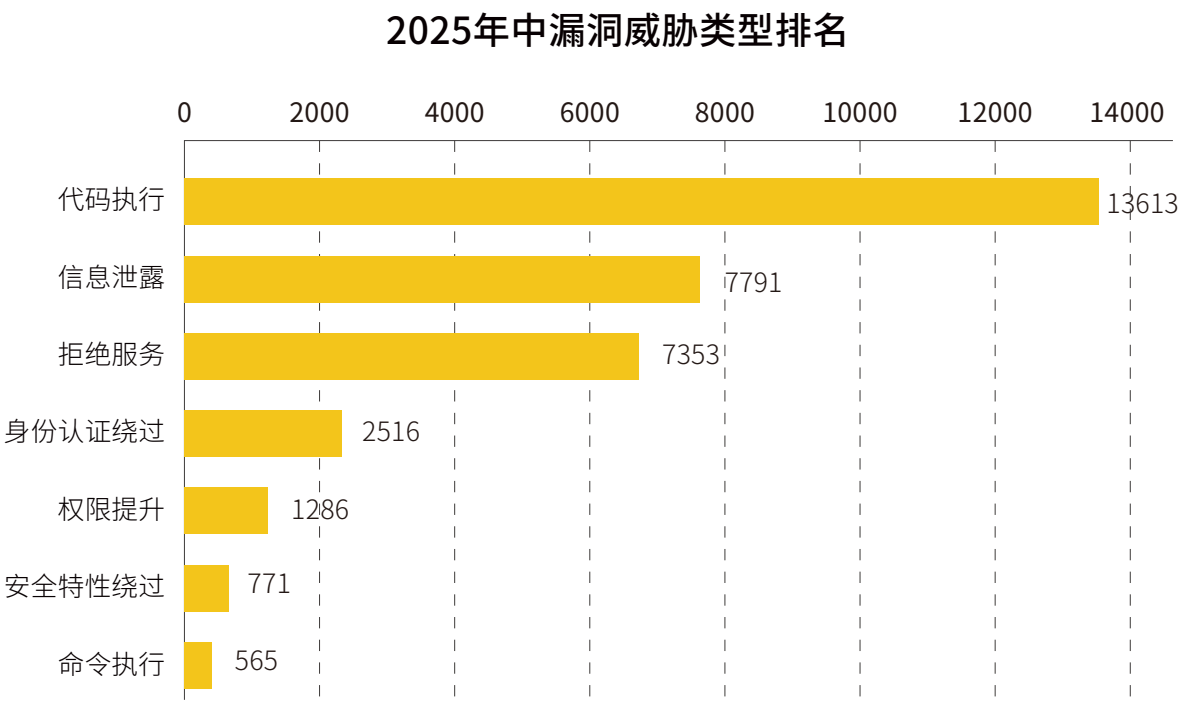
2025上半年漏洞数量呈现稳定增长态势，截至6月，新增漏洞数量达到23351个，较去年同期增长14.0%。这一增长趋势延续了近年来漏洞数量持续上升的态势，反映出随着技术生态的日益复杂，软件和系统中潜藏的安全隐患不断被挖掘出来。

奇安信漏洞情报页面：https://ti.qianxin.com/vulnerability/list
漏洞风险通告发布页面：https://ti.qianxin.com/vulnerability/notice-list
漏洞深度分析报告发布页面：https://ti.qianxin.com/vulnerability/deep-analysis-report

二、漏洞类型分布与威胁分析

代码执行、信息泄露和权限提升依然是攻击者利用的漏洞核心类型，这一点和去年保持一致。

对2025上半年新增的漏洞信息根据漏洞威胁类型进行分类总结，如图1-2所示：



△图1-2 漏洞威胁类型排名

其中漏洞数量占比最高的前三种类型分别为：代码执行、信息泄露、拒绝服务。RCE 漏洞由于其极高的危害性，一直是攻击者重点关注的对象。在 2025 年上半年，多个关键应用系统和中间件被曝出 RCE 漏洞。攻击者可通过构造特定请求，在未授权的情况下远程执行任意代码，获取系统权限。此类漏洞的爆发，凸显了应用系统在输入验证、权限控制等方面存在的薄弱环节。SQL 注入漏洞在上半年依然频发，主要集中在国产 OA 系统、企业资源规划（ERP）系统等。据统计，上半年因 SQL 注入漏洞导致的数据泄露事件达40件起，给企业带来了巨大的经济损失和声誉影响。

三、漏洞影响厂商与行业分布

将2025上半年新增的23351个条漏洞信息根据漏洞影响厂商进行分解，如图1-3所示：

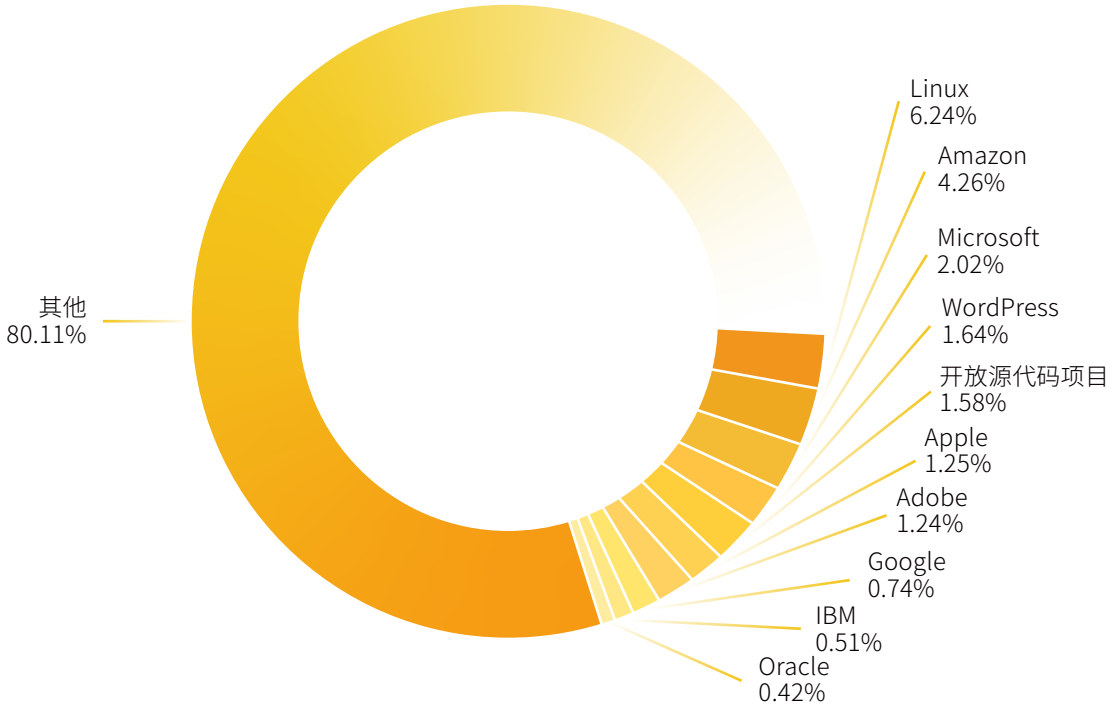


图1-3 漏洞影响厂商占比

其中漏洞数量占比最高的前十家厂商为：Linux、Amazon、Microsoft、WordPress、开放源代码项目、Apple、Adobe、Google、IBM、Oracle。Linux、Microsoft、Apple这些厂商漏洞多发，且因为其有节奏的发布安全补丁，必然成为漏洞处置的关注重点。开源软件和应用在企业中被使用的越来越多，关注度逐渐攀升。部署在网络边界的网络设备在攻防行动中占据了重要地位，因而获得了安全研究员的重点关注。

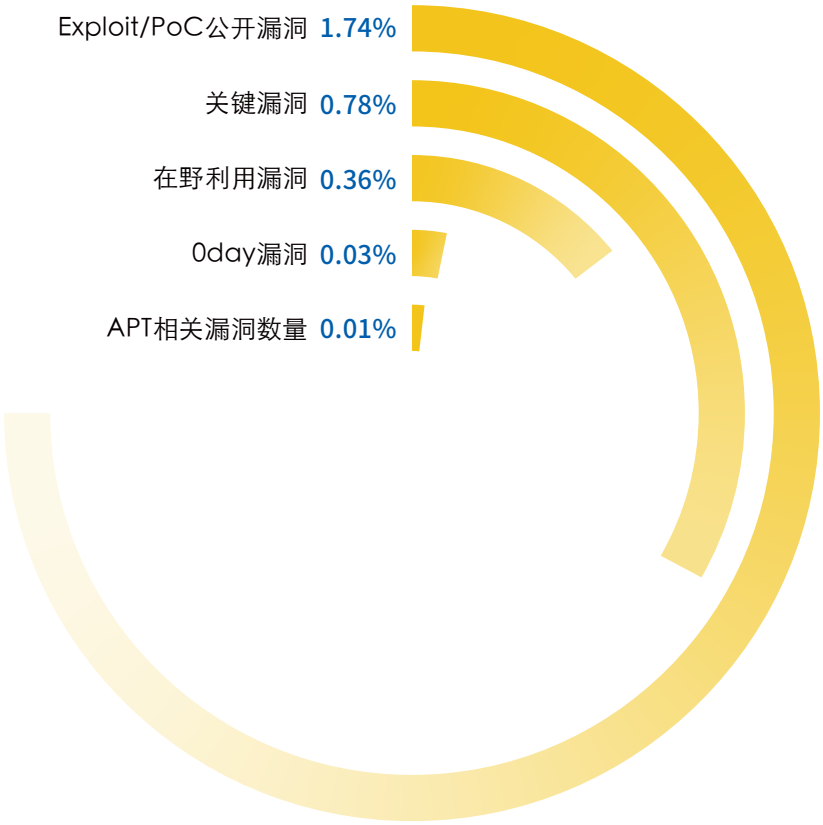
2025年中新增的漏洞中，有218个在NVD上没有相应的CVE编号，未被国外漏洞库收录，为国产软件漏洞，占比情况如图1-4所示。这些漏洞在OA和网络设备中尤为突出。受影响行业包括：政府机构（APT攻击的首要目标）、金融领域（高危漏洞利用频发）、能源与关键基础设施（攻击者重点关注的领域）。此类漏洞具有较高威胁，如果被海外国家背景攻击组织利用将导致非常严重的安全后果。

△图1-4 国产软件漏洞占比

四、关键漏洞占比情况

奇安信将0day、APT相关、发现在野利用、存在公开Exploit/PoC，且漏洞关联软件影响面较大的漏洞标记为“关键漏洞”。此类漏洞的技术细节或验证利用代码已在互联网上被公开，或已经发现在野攻击利用，且漏洞关联产品具有较大的影响面，综合来看威胁程度相对较高，需要重点关注。

2025年中奇安信CERT共标记关键漏洞182个，占2025上半年新增漏洞的0.78%；存在公开Exploit/PoC漏洞数量为407个，占2025上半年新增漏洞的1.74%；发现已有在野利用漏洞数量为86个，占2025上半年新增漏洞的0.36%；0day漏洞数量为7个，占2025上半年新增漏洞的0.03%；APT相关漏洞数量为1个，占2025上半年新增漏洞的0.01%。上述各类漏洞在2025年中新增漏洞中占比情况如图1-5所示：



△图1-5 各类关键漏洞在全年新增漏洞中占比情况

五、漏洞标签占比情况

为了更加有效的管控漏洞导致的风险，奇安信漏洞情报建立了全面的多维漏洞信息整合及属性标定机制，使用“关键漏洞”、“在野利用”、“POC公开”、“影响量级”、“Botnet类型”、“攻击者名称”、“漏洞别名”等标签，标定漏洞相关的应用系统部署量、是否已经有了公开的技术细节、Exploit工具、概念验证代码（PoC）、是否已经出现野外利用、是否已经被已知的漏洞利用攻击包或大型的Botnet集成作为获取对系统控制途径等属性。涵盖的漏洞标签类别如图1-6所示：

图1-6 漏洞标签词云图

六、漏洞热度排名TOP 10

根据奇安信CERT全面的漏洞信息监测数据，总结2025上半年漏洞舆论热度榜TOP 10漏洞如下：

排名	漏洞名称	漏洞编号	危险等级	修复建议
1	Apache Tomcat 远程代码执行漏洞	CVE-2025-24813	高危	建议用户尽快升级至最新版本： Apache Tomcat >=11.0.3、Apache Tomcat >=10.1.35、Apache Tomcat >=9.0.99
2	Windows 文件资源管理器欺骗漏洞	CVE-2025-24071	高危	安装补丁
3	Foxmail for Windows 远程代码执行漏洞	QVD-2025-13936	高危	现 Windows Foxmail官网 (https://www.foxmail.com/win) 已更新，所有受影响 Windows 用户均可通过自动更新机制或手动升级到最新版完成安全修复。
4	Google Chrome 越界读写漏洞	CVE-2025-5419	高危	建议用户尽快升级至最新版本： Google Chrome(Windows/Mac) >= 137.0.7151.68/.69、Google Chrome(Linux) >= 137.0.7151.68
5	Google Chrome 沙箱逃逸漏洞	CVE-2025-2783	高危	建议用户尽快升级至最新版本： Google Chrome(Windows) >= 134.0.6998.177/.178
6	Windows SMB 权限提升漏洞	CVE-2025-33073	高危	安装补丁
7	VMware ESXi 多个高危漏洞	CVE-2025-22224 CVE-2025-22225 CVE-2025-22226	高危	建议用户尽快升级至最新版本： VMware ESXi 8.0 >= ESXi80U3d-24585383\ESXi80U2d-24585300、VMware ESXi 7.0 >= ESXi70U3s-24585291、VMware Workstation 17.x >= 17.6.3、VMware Fusion 13.x >= 13.6.3、VMware Cloud Foundation 5.x >=异步补丁 ESXi80U3d-24585383、VMware Cloud Foundation 4.5.x >=异步补丁 ESXi70U3s-24585291、VMware Telco Cloud Platform 5.x, 4.x, 3.x, 2.x >= KB389385、VMware Telco Cloud Infrastructure 3.x, 2.x >= KB389385
8	Zabbix groupBy SQL 注入漏洞	CVE-2024-36465	高危	建议受影响用户升级至最新版本： Zabbix 7.0.* >= 7.0.8rc2、Zabbix 7.2.* >= 7.2.2rc1、Zabbix 7.4.0alpha1
9	Ingress NGINX Controller 远程代码执行漏洞	CVE-2025-1974	高危	建议受影响用户升级至最新版本： ingress-nginx v1.12.1、ingress-nginx v1.11.5
10	Linux 本地提权漏洞利用链	CVE-2025-6018 CVE-2025-6019	高危	官方已发布修复版本，openSUSE Leap 15 和 SUSE Linux Enterprise 15 用户应立即更新 PAM 相关组件；官方已发布 libblockdev 漏洞修复版本，用户应根据使用的系统类型进行更新。

在上半年总热度舆论榜前十的漏洞中，热度最高的漏洞为Apache Tomcat 远程代码执行漏洞(CVE-2025-24813)。当应用程序DefaultServlet启用写入功能（默认情况下禁用）、使用 Tomcat默认会话持久机制和存储位置、依赖库存在反序列化利用链时，未授权攻击者能够执行恶意代码获取服务器权限。鉴于该漏洞影响范围较大，建议受影响用户升级至Apache Tomcat v11.0.3、v10.1.35、v9.0.99。

七、2025年中最危险的CWE类型

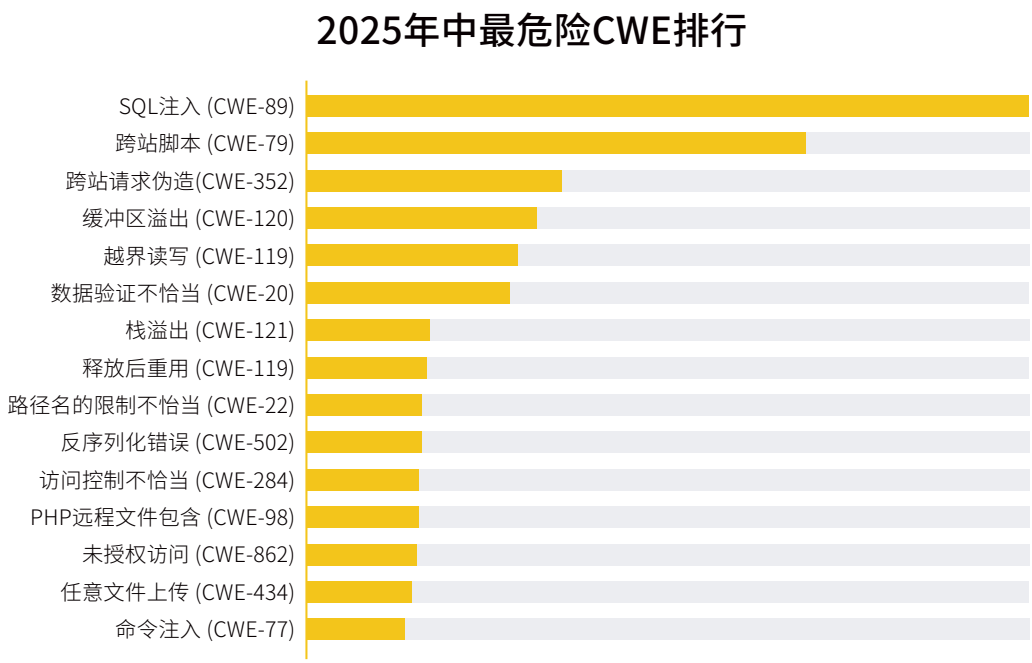
CWE 是代码、设计或架构中可能导致漏洞的常见软件弱点或缺陷的列表，它们本身列在常见漏洞和披露（CVE）数据库中。某些漏洞通常很容易找到并加以利用，攻击者通过这些漏洞能够窃取数据、完全接管系统或阻止应用程序运行。CWE 是这些漏洞的根本原因。

为了定义软件弱点的严重性级别，2025上半年，奇安信CERT汇集本年度9880个高危、极危漏洞，从中总结出最危险 CWE 列表供参考。2025年中最危险CWE排行如图1-7所示，该排名不仅为开发人员和安全专业人员提供了可靠信息，还为企业和公司提供了安全战略指南。

在9880个高危、极危漏洞中，SQL 注入，也称为“SQL命令中使用的特殊元素转义处理不恰当”（CWE-89）占据首位，有1502个漏洞，占总数的15.20%。SQL 注入在2025年上半年仍然是一种重要且具有严重威胁的网络安全问题。

跨站脚本，也称为“在Web页面生成时对输入的转义处理不恰当”（CWE-79）位居第二，有1040个漏洞，在2025年中占据核心地位，其重要性主要体现在攻击范围广泛性、与其他高危漏洞的连锁效应、防护难度等方面，占总数的10.53%。

第三名是跨站请求伪造（CWE-352），有532个漏洞，占总数的5.38%。



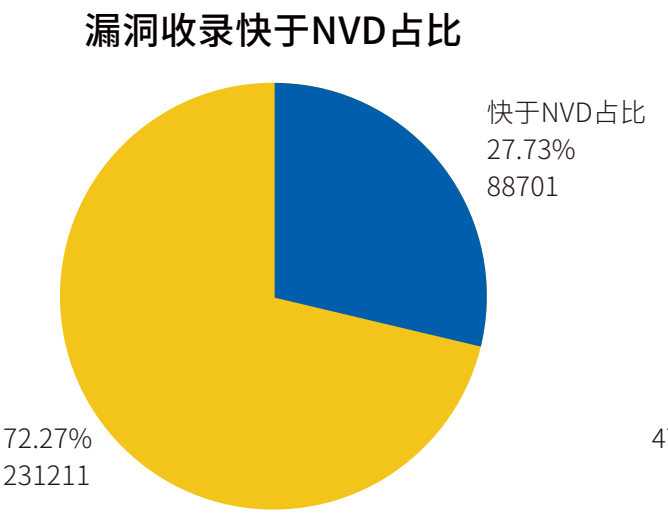
△图1-7 2025年中最危险CWE排行

建议查看此列表并通过它获悉软件安全策略。在开发和采购流程中优先考虑这些弱点有助于防止软件生命周期核心的漏洞。

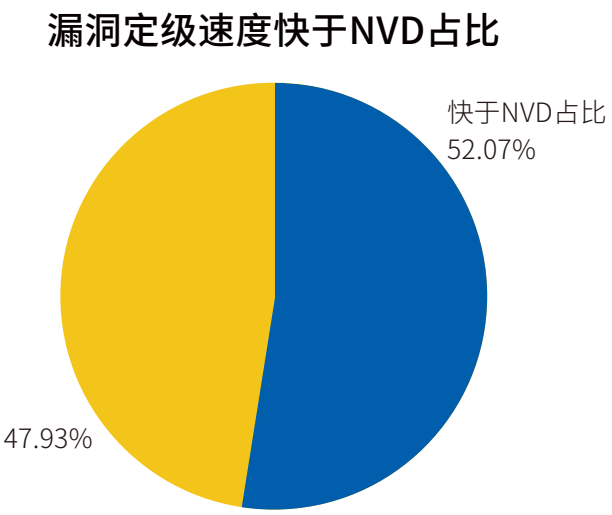
八、漏洞修复时效性

2025上半年漏洞平均修复时间：39.6天，较2024年缩短12%。零日漏洞修复不足：7个零日漏洞中40%修复时间超过20天，部分漏洞已在披露前被利用。披露与利用时间差：公开后3天内被利用的漏洞占50%。

值得注意的是，2025上半年新增漏洞中，有23351个漏洞存在CVE编号，其中有23121个存在CVE的漏洞，在NVD（National Vulnerability Database，美国国家漏洞数据库）收录前已被奇安信CERT通过第一手信息源的监控发现并收录，占本年度存在CVE漏洞总数的27.7%，且漏洞平均定级速度快于NVD约52.1%。这些漏洞通过奇安信CERT多源汇聚技术，在厂商发布安全通告的第一时间即可捕获漏洞信息，由分析人员研判入库。快于NVD占比如图1-8、图1-9所示：



△图1-8 漏洞收录快于NVD占比



△图1-9 漏洞定级速度快于NVD占比

漏洞发现的时效性在网络安全领域至关重要，它直接影响到组织和个人的数据安全、业务连续性和声誉。漏洞发现得越早，攻击者利用该漏洞进行攻击的时间窗口就越小。及时的漏洞发现可以减少攻击者利用漏洞的机会。一旦确认资产存在相关的漏洞，组织可以迅速采取行动，如打补丁、更新系统或采取临时的缓解措施，以阻止潜在的攻击。及时修复漏洞可以减少数据泄露、服务中断和其他安全事件造成的损害，从而降低相关的财务成本和声誉损失。

02 第二章

重大漏洞案例分析

本章节梳理了2025上半年影响较大网络安全事件中关联的高危漏洞，这些漏洞已经被威胁行为体用于发起网络攻击，部分漏洞利用代码已在互联网上被公开，威胁程度极高，需要重点关注、优先修补。基于威胁情报的漏洞处理优先级排序对于威胁的消除能够起到事半功倍的效果。

一、Apache Tomcat 管理面板遭受黑客组织定向暴力攻击

事件描述

6月5日开始，GreyNoise 分析师发现了两个针对 Apache Tomcat Manager 界面的暴力攻击活动，并试图通过 Internet 访问 Tomcat 服务。

默认情况下，Tomcat Manager 配置为仅允许来自 localhost（127.0.0.1）的访问，没有预配置的凭据和远程访问。但是当在线暴露时，Web 应用程序可能会成为攻击者的目标。第一个使用近 300 个唯一的 IP 地址，其中大多数被标记为恶意，这些地址试图登录在线暴露的内容，第二个使用 250 个恶意 IP 以 Tomcat Manager Web 应用程序为目标进行暴力攻击，威胁行为者使用自动化工具测试数千甚至数百万个可能的凭据。

研究人员表示，这种攻击执行起来非常简单，不需要身份验证。唯一的要求是 Tomcat 使用基于文件的会话存储，这在许多部署中很常见。更糟糕的是，base64 编码允许漏洞绕过大多数传统的安全过滤器，使检测变得具有挑战性。

主动利用已在全球范围内观察到，攻击者主要针对美国、日本、印度、韩国和墨西哥的系统。

关联漏洞

1. Apache Tomcat 远程代码执行漏洞(CVE-2025-24813)

受影响版本	11.0.0-M1 <= Apache Tomcat <= 11.0.2 10.1.0-M1 <= Apache Tomcat <= 10.1.34 9.0.0.M1 <= Apache Tomcat <= 9.0.98
影响量级	千万级
危害描述	未授权攻击者能够执行恶意代码获取服务器权限。
修复措施	禁止partial PUT：在 conf/web.xml 中修改 allowPartialPut 参数为false，并重启 Tomcat 以使配置生效。 严格控制 DefaultServlet 写入权限：确保 readonly=true，禁用所有未经授权的 PUT/DELETE 请求，仅允许可信来源访问受限目录。 检查应用程序依赖库。

二、黑客利用 Windows WebDav 零日漏洞投放恶意软件

事件描述

一个名为“Stealth Falcon”的 APT 黑客组织自2025年3月起利用 Windows WebDav RCE 漏洞对土耳其、卡塔尔、埃及和也门的国防和政府组织发动零日攻击。Stealth Falcon（又名“FruityArmor”）是一个高级持续性威胁 (APT) 组织，以对中东组织进行网络间谍攻击而闻名。

当 .url 文件将其 WorkingDirectory 设置为远程 WebDAV 路径时，内置的 Windows 工具可能会被诱骗从该远程位置而不是合法位置执行恶意可执行文件。
这使得攻击者可以强制设备从他们控制的 WebDAV 服务器远程执行任意代码，而无需在本地删除恶意文件，从而使他们的操作变得隐秘且难以捉摸。

关联漏洞

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

受影响版本	Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows Server 2025 (Server Core installation) Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems 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 Server 2016 (Server Core installation) Windows Server 2016 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 Server 2025 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems
影响量级	千万级
危害描述	远程攻击者可以诱骗受害者点击特制链接，并在系统上执行任意代码。
修复措施	官方已发布安全更新补丁，受影响用户可以到官方下载对应的补丁更新， 或者手动更新系统 。

三、2025年第一个 Chrome 零日漏洞在间谍活动中被利用

事件描述

谷歌修复了一个高危 Chrome 零日漏洞，该漏洞可导致攻击者逃离浏览器沙盒并在针对俄罗斯媒体和教育机构的间谍攻击中部署恶意软件。该安全漏洞正被用于网络钓鱼攻击，将受害者重定向到 prima-kovreadings[.]info 域，这是针对俄罗斯组织的网络间谍活动的一部分，该活动被称为 Operation ForumTroll。

此漏洞由卡巴斯基实验室的 Boris Larin和Igor Kuznetsov 发现，他们将其描述为“Windows 上 Mojo 在未指定情况下提供的错误句柄”。发现该零日漏洞的卡巴斯基研究人员也发布了一份包含更多细节的报告，称攻击者利用 CVE-2025-2783 漏洞绕过 Chrome 沙盒保护，并使用复杂的恶意软件感染目标。

关联漏洞

1. Google Chrome沙箱逃逸漏洞(CVE-2025-2783)

受影响版本	Google Chrome(Windows) < 134.0.6998.177/.178
影响量级	千万级
危害描述	攻击者可利用该漏洞绕过沙箱隔离机制，造成信息泄露、代码执行等危害。
修复措施	目前官方已发布安全更新，建议用户尽快升级至最新版本： Google Chrome(Windows) >= 134.0.6998.177/.178

四、披露闹剧给 CrushFTP 漏洞利用蒙上阴影

事件描述

Shadowserver基金会报告称，针对CrushFTP文件传输服务器软件中一个高危身份验证绕过漏洞CVE-2025-2825的攻击活动正在进行中。截至3月31日，Shadowserver的扫描显示，存在1,512个易受攻击的CrushFTP实例，攻击者利用了几天前发布的概念验证（PoC）漏洞进行攻击。

该漏洞允许攻击者绕过身份验证，并通过暴露的 HTTP(S) 端口访问文件传输服务器。安全研究人员表示，该漏洞的 CVSS 评分为 9.8，因为它可以远程执行且易于利用。

关联漏洞

1.CrushFTP 服务器端认证绕过漏洞(CVE-2025-31161)

受影响版本	CrushFTP v10 CrushFTP v11
影响量级	万级
危害描述	攻击者可以通过构造特殊的 HTTP Authorization 请求头，获得系统完全控制权。
修复措施	1.立即升级: 将 CrushFTP 升级至 v10.8.4 或 v11.3.1 及以上版本。 2.验证修补状态: 确保所有实例均已应用补丁。 3.监控异常活动: 检查系统日志中是否存在异常登录或会话活动。

五、知名前端工具vite接连曝出4个任意文件读取漏洞

事件描述

2025年3月，知名前端开源工具Vite接连曝出4个任意文件读取漏洞。该系列漏洞是由于Vite开发服务器的文件访问控制机制存在缺陷且补丁修复不够全面，导致攻击者通过不同参数组合、路径构造或特殊字符屡次绕过server.fs.deny限制，非法访问项目根目录外的敏感文件。Vite广泛应用于Vue.js项目开发，在国内有十万级的暴露风险资产，建议用户尽快做好自查及防护。

关联漏洞

1. Vite 任意文件读取漏洞(CVE-2025-30208)

受影响版本	6.2.0 <= Vite <= 6.2.2 6.1.0 <= Vite <= 6.1.1 6.0.0 <= Vite <= 6.0.11 5.0.0 <= Vite <= 5.4.14 Vite <= 4.5.9
影响量级	十万级
危害描述	攻击者可利用该漏洞获取源码、SSH 密钥、数据库账号、用户数据等敏感信息，可能导致系统数据泄露等严重后果。
修复措施	建议受影响用户升级至最新版本：Vite 6.2.3、6.1.2、6.0.12、5.4.15、4.5.10。通过限制开发服务器的访问权限，如关闭 server.host 或将其绑定到特定的 IP 地址，以减少攻击面。

2. Vite 任意文件读取漏洞(CVE-2025-31125)

受影响版本	6.2.0 <= Vite <= 6.2.3 6.1.0 <= Vite <= 6.1.2 6.0.0 <= Vite <= 6.0.12 5.0.0 <= Vite <= 5.4.15 Vite <= 4.5.10
影响量级	十万级
危害描述	攻击者可利用该漏洞获取源码、SSH 密钥、数据库账号、用户数据等敏感信息，可能导致系统数据泄露等严重后果。
修复措施	建议受影响用户升级至最新版本：Vite 6.2.4、6.1.3、6.0.13、5.4.16、4.5.11。通过限制开发服务器的访问权限，如关闭 server.host 或将其绑定到特定的 IP 地址，以减少攻击面。

3. Vite 任意文件读取漏洞(CVE-2025-31486)

受影响版本	6.2.0 <= Vite <= 6.2.4 6.1.0 <= Vite <= 6.1.3 6.0.0 <= Vite <= 6.0.13 5.0.0 <= Vite <= 5.4.16 Vite <= 4.5.11
影响量级	十万级
危害描述	攻击者可利用该漏洞获取源码、SSH 密钥、数据库账号、用户数据等敏感信息，可能导致系统数据泄露等严重后果。
修复措施	建议受影响用户升级至最新版本：Vite 6.2.5、6.1.4、6.0.14、5.4.17、4.5.12。通过限制开发服务器的访问权限，如关闭 server.host 或将其绑定到特定的 IP 地址，以减少攻击面。

4. Vite 任意文件读取漏洞(CVE-2025-32395)

受影响版本	6.2.0 <= Vite <= 6.2.5 6.1.0 <= Vite <= 6.1.4 6.0.0 <= Vite <= 6.0.14 5.0.0 <= Vite <= 5.4.17 Vite <= 4.5.12
影响量级	十万级
危害描述	攻击者可利用该漏洞获取源码、SSH 密钥、数据库账号、用户数据等敏感信息，可能导致系统数据泄露等严重后果。
修复措施	建议受影响用户升级至最新版本：Vite 6.2.6、6.1.5、6.0.15、5.4.18、4.5.13。通过限制开发服务器的访问权限，如关闭 server.host 或将其绑定到特定的 IP 地址，以减少攻击面。

六、严重“IngressNightmare”漏洞危及 Kubernetes 环境

事件描述

Kubernetes 的维护人员已经发布了针对 Ingress NGINX 控制器中四个严重漏洞的补丁，这些漏洞影响了 6,500 个（占所有面向互联网的容器编排集群的 41%），其中包括多家财富 500 强公司使用的集群。

这些漏洞允许远程、未经身份验证的攻击者在受影响的环境中执行任意命令并完全接管 Kubernetes 集群。其中三个漏洞（CVE-2025-24514、CVE-2025-1097 和 CVE-2025-1098）允许攻击者在受影响的系统上注入任意 NGINX 配置指令，包括自定义路由规则和安全设置。然而，要实现远程代码执行，攻击者需要将这三个漏洞中的任何一个与第四个漏洞 CVE-2025-1974 组合使用。

这四个漏洞具体影响了 NGINX Controller for Kubernetes 的准入控制器组件，该组件负责在 API 服务器处理传入的 Ingress 对象和其他资源之前对其进行验证和/或修改。CVE-2025-1974 意味着 Pod 网络上的任何东西都很有可能接管你的 Kubernetes 集群，而无需任何凭证或管理访问权限。在许多常见情况下，云 VPC 中的所有工作负载，甚至任何连接到公司网络的人，都可以访问 Pod 网络！这是一个非常严重的情况。

关联漏洞

1. Ingress NGINX Controller 远程代码执行漏洞(CVE-2025-1974)

受影响版本	ingress-nginx <= 1.12.0 ingress-nginx <= 1.11.4
影响量级	万级
危害描述	攻击者利用此漏洞可远程执行代码，获取集群中的敏感信息，甚至完全控制集群。
修复措施	将 ingress-nginx 升级到 v1.11.5、v1.12.1 或任何更高版本。升级之前，可以通过将“enable-annotation-validation”CLI 参数设置为“true”来缓解此漏洞。

03

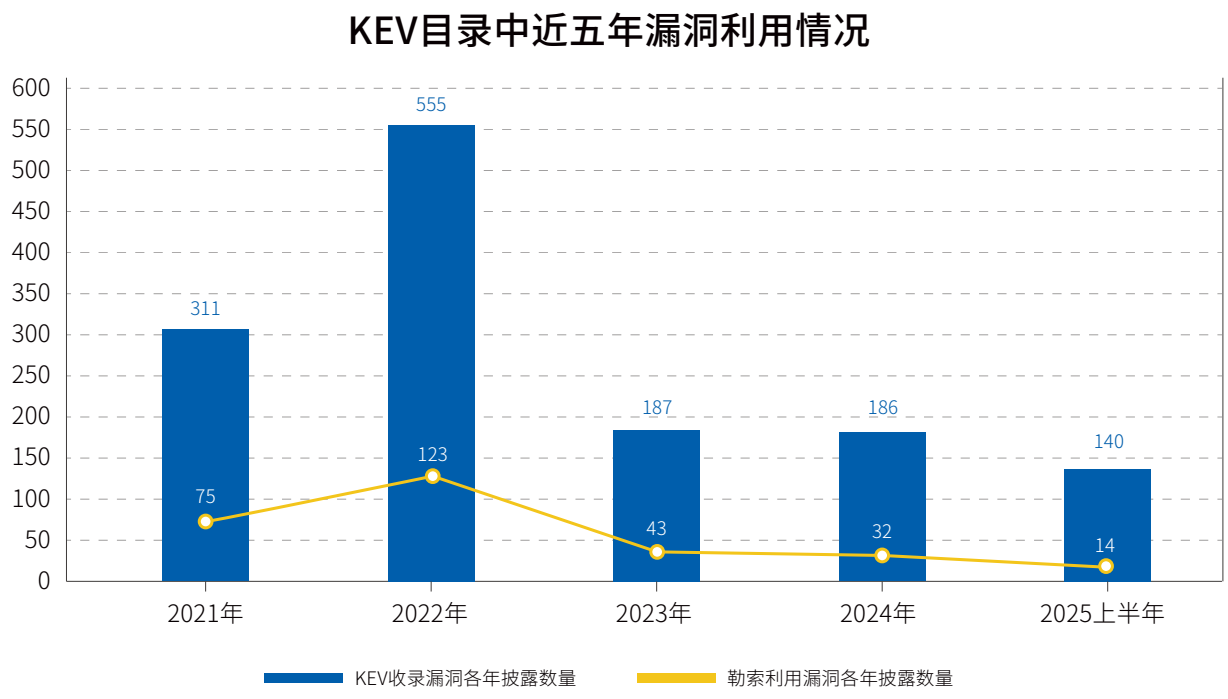
第三章

关键种类漏洞分析

一、漏洞利用情况及趋势

2021年，美国把“漏洞已被公开利用”视为对网络安全的头号威胁，并为此设立了“已知被利用漏洞”清单（Known Exploited Vulnerabilities，KEV）。该清单要求所有联邦机构优先修补这些漏洞，从而迅速削减现实攻击面。由于这一做法行之有效，KEV清单很快成为全球公认的“已被野外利用漏洞”风向标，帮助各类组织在漏洞修复时确定轻重缓急。以下结合KEV及奇安信CERT漏洞库数据对近5年漏洞利用情况分析，并对2025年下半年漏洞态势进行预测。

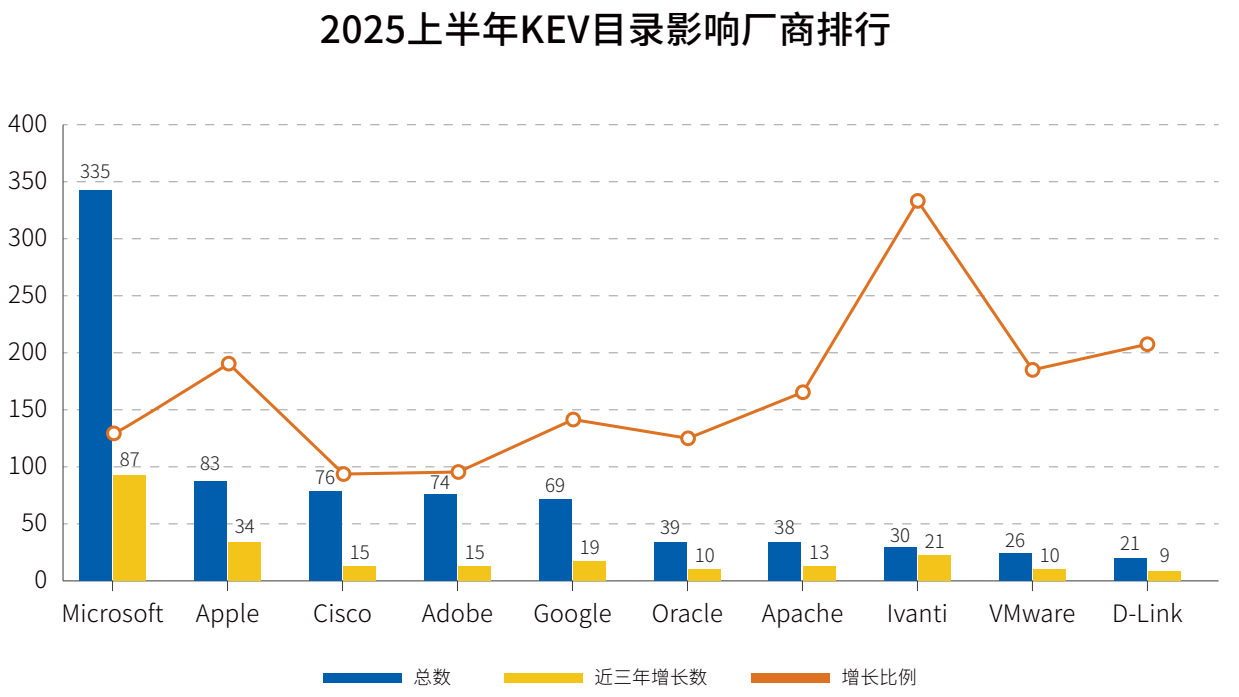
近5年漏洞利用总量呈“倒V”型，2022触顶后连续三年回落。2025上半年数据显示存量风险趋稳，但0day隐蔽化、移动化、供应链化三大趋势明显。对KEV目录中漏洞CVE编号年份进行统计发现，2022年漏洞利用数量达到峰值。在2022年以前漏洞利用总数呈上升趋势，2022年为历史顶峰，随后三年连续下滑，2025 H1总量已不足2022年的60%。直至25年上半年，漏洞治理初见成效，预计2025下半年KEV收录总量小幅反弹，但勒索利用继续“质大于量”。CISA将统筹漏洞治理作为重要任务，通过协同漏洞披露（CVD）、漏洞披露策略（VDP）、相关约束性操作指令（BOD）等一系列措施的执行，加之厂商对漏洞的重视，历史存量漏洞被快速收敛。KEV目录中近五年漏洞利用情况如图3-1所示：



△图3-1 KEV目录中近五年漏洞利用情况

截至2025年上半年，KEV目录中已知被勒索软件利用漏洞共287个，其数量变化与整体趋势一致，在2022年达到峰值。随着全球范围内对勒索软件大型组织的追踪打击，勒索软件利用漏洞数量同步下降，这一变化得益于国际执法机构的协同整治，但勒索软件攻击仍是威胁主力。随着全球范围对勒索组织的打击，勒索组织为提高攻击效率可能会优先考虑使用能够有效提供访问权限的漏洞开展攻击。

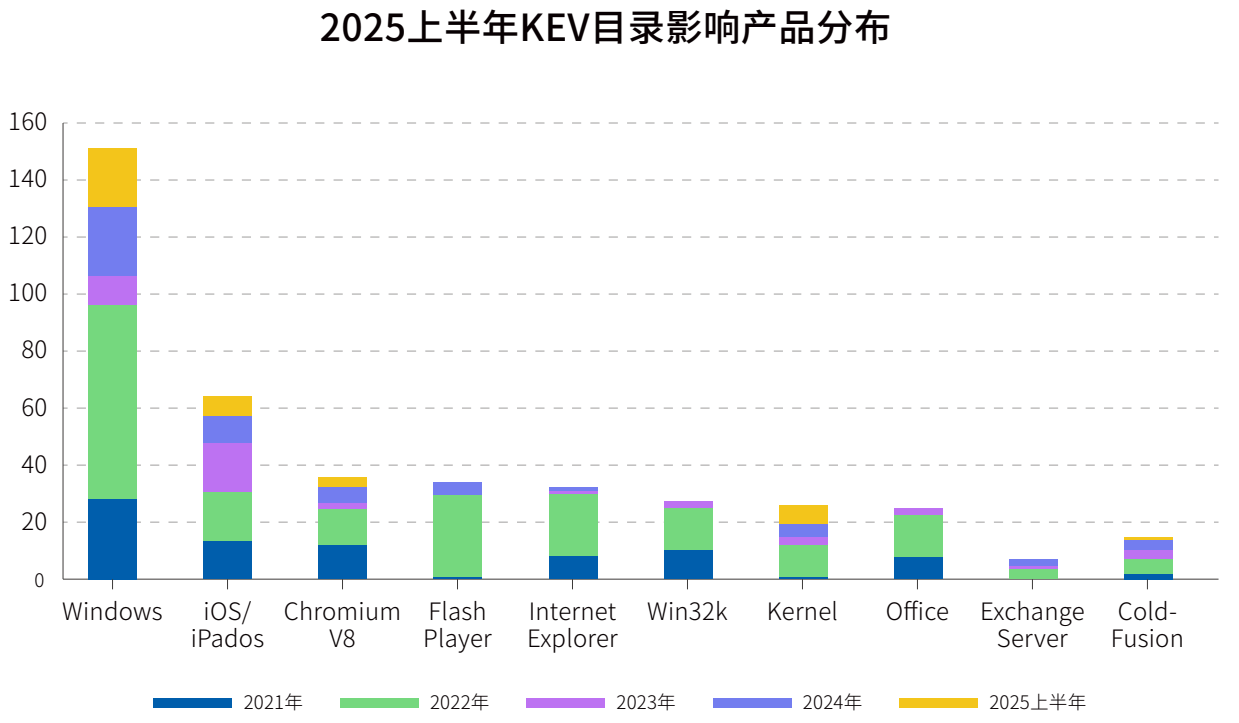
对截止2025上半年KEV目录收录的1379个漏洞进行分析，受影响厂商排行前十情况如图3-2所示。2025上半年，KEV目录收录漏洞140个，Microsoft和 Apple的漏洞最多，其主要受影响产品分别为Windows操作系统和iOS/iPadOS。



△图3-2 2025上半年KEV目录影响厂商排行

从全部收录数据来看，Microsoft 被利用情况最严重，已知被利用漏洞数量高达335个，其次分别为 Apple（83个）、Cisco（76个）、Adobe（74个）、Google（63个）。从增长趋势来看，Apple、Ivanti、Google 增长明显，Ivanti三年间增长70%以上。而Cisco、Adobe、Oracle、Apache等近年来被利用漏洞情况有所缓解，其CVE编号在2022年及以前的漏洞被利用情况相对严重。

从影响产品情况来看，见图3-3所示，2022年已知被利用漏洞数量达到峰值，成为了漏洞趋势变化的一个关键点。2025上半年，奇安信CERT监测发现，受影响最大的产品仍是操作系统和浏览器，将持续影响2025下半年。



△图3-3 2025上半年KEV目录影响产品分布

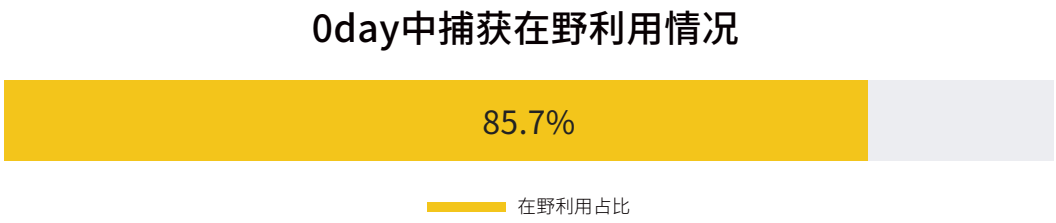
Microsoft的Windows操作系统已知被利用漏洞最多，且近几年保持稳定增长趋势。Win32k作为Windows操作系统内核中的一个关键组件，被利用情况集中在2022年及以前。Exchange Server存在多个高危0day漏洞在2021年和2022 年被广泛利用，对全球范围的用户造成了严重威胁。直至2024年Exchange Server和相关组件漏洞仍然是攻击者重点关注的对象。

近年来主流浏览器使用情况的转变，导致浏览器漏洞利用重心从Internet Explorer转变为Google Chrome。Internet Explorer作为以前的主流浏览器，存在大量历史被利用漏洞，但在2022年后新的被利用漏洞数量趋近于0。Chromium V8浏览器引擎被利用漏洞在2021年开始快速增长，之后每年被利用漏洞的占比都保持相对稳定。也深受攻击者和APT组织的“青睐”。

二、0day漏洞

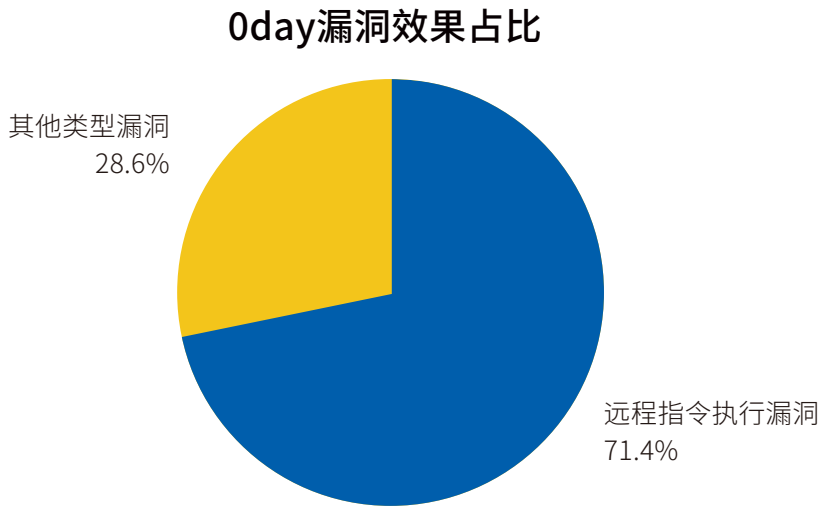
0day漏洞攻击已成为黑客常规武器，奇安信CERT在2025上半年新增收录 0day漏洞7个，其中被捕获到在野利用活动的占比85.7%，57.1%的漏洞发现公开Exploit/PoC。近1/3发现在野利用的0day漏洞没有监测到公开的利用代码，处于私有状态，仅被某些APT组织或者个人使用。但厂商对于漏洞修复的平均时长要1-2周，缩短和攻击者掌握0day漏洞的时间差迫在眉睫。

本章节回顾了2025上半年部分影响较大的0day漏洞，有6个0day已经捕获到在野利用行为，占比85.7%,如图3-4所示。这足以显示0day杀伤力强、极难防范，是威胁行为体最好的攻击武器。



△图3-4 0day中捕获在野利用占比

在调查本年度影响重要的7个0day漏洞中，能够实现远程指令执行的漏洞或组合漏洞占比71.4%，占据过半，这类漏洞通常危害程度最高，可以被用来完全控制受影响的系统。0day漏洞效果占比如图3-5所示：



△图3-5 0day漏洞效果占比

1、Craft CMS 远程代码执行漏洞

2025年2月中旬，Orange Cyberdefense团队在排查某Craft CMS服务器日志过程中发现未授权远程代码执行漏洞(CVE-2025-32432)。
2025年4月10日,Craft CMS官方发布修复版本并提醒用户存在在野利用。
2025年4月18日，Orange Cyberdefense SensePost发布文章包括技术细节和POC。

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-32432	十万级	代码执行	10.0	是	已公开	已公开	已发现

Craft CMS 远程代码执行漏洞源于其generate-transform功能在处理用户输入时存在反序列化缺陷，结合Yii框架的输入验证漏洞（CVE-2024-58136），未授权攻击者可构造恶意HTTP请求，执行任意代码完全控制服务器。

2、Ivanti Endpoint Manager Mobile远程代码执行漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-4427	万级	身份认证绕过	5.3	是	已公开	已公开	已发现
CVE-2025-4428		代码执行	7.2	是	已公开	已公开	已发现

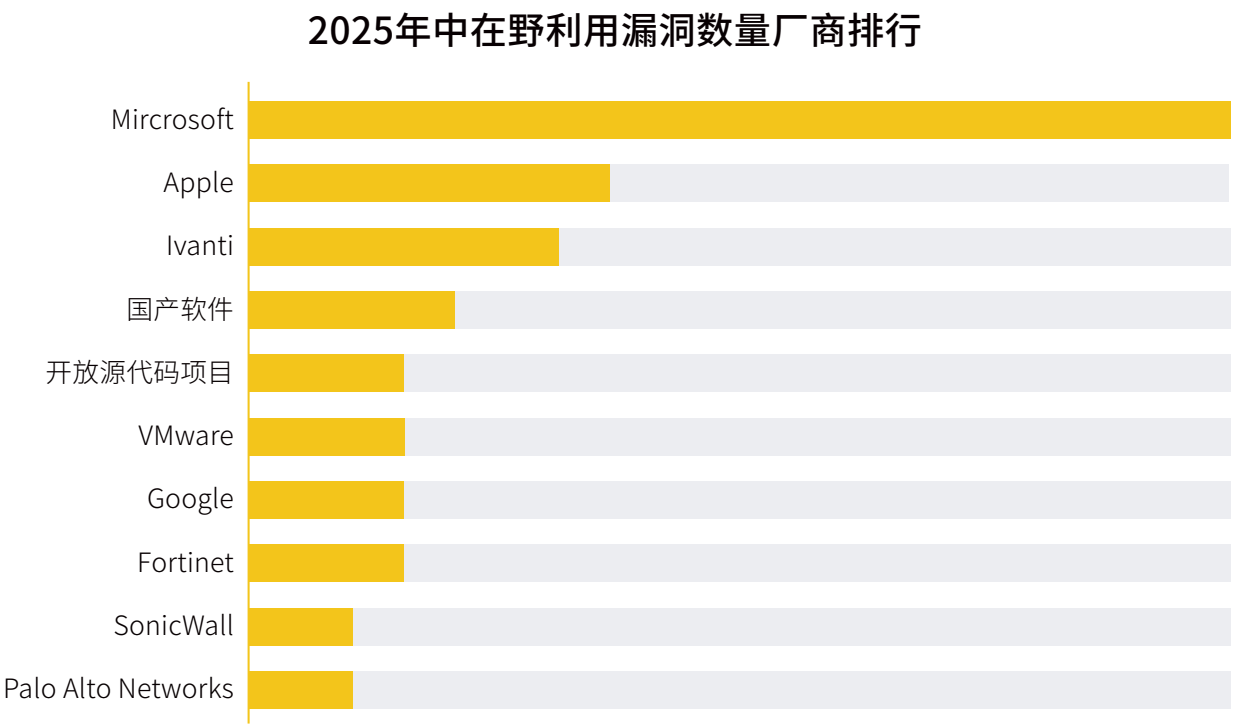
Ivanti Endpoint Manager Mobile（EPMM）是一款企业级的移动设备管理解决方案，用于集中管理和保护企业中的移动设备，支持设备注册、应用分发、安全策略实施等功能，帮助企业确保移动设备的安全性和合规性。
2025年5月13日，Ivanti披露Endpoint Manager Mobile(EPMM)漏洞利用链(CVE-2025-4427、CVE-2025-4428)，这两个漏洞源于对Java表达式语言的不安全使用以及路由配置错误，可以组合利用实现未经身份验证的远程代码执行。官方确认在披露前有极少数客户遭到了攻击。
2025年5月16日，在POC公开后，Wiz确认这些漏洞在被广泛利用。

三、在野利用相关漏洞

奇安信多款产品具有漏洞在野攻击的发现能力，基于自有数据的视野可以观察到大量APT组织、黑产团伙的攻击活动，能够及时获取漏洞的在野利用情况。在2025上半年，奇安信监测到以下数据：

1.监测到漏洞被实际利用	2.漏洞利用行为超过	3.捕获到攻击IP数量约
500+个	1000万次	40万个

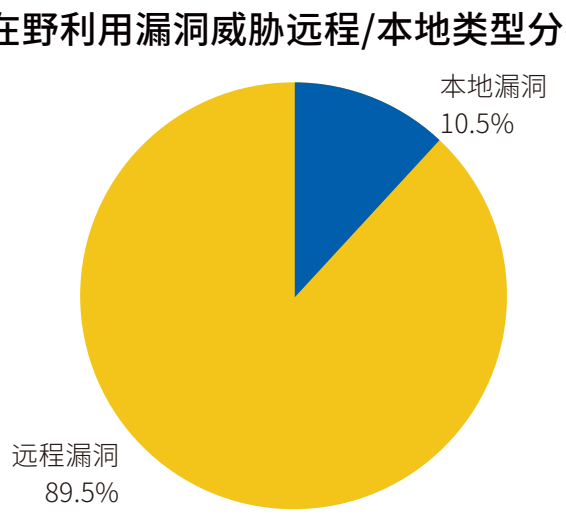
在这500+个被实际利用的漏洞中，2025上半年新暴露的有86个，涉及广泛的操作系统和应用程序，排名前十位的分别是Mircrosoft、Apple、Ivanti、国产软件、Fortinet、Google、VMware、开放源代码项目、Palo Alto Networks、SonicWall。2025上半年在野利用漏洞数量厂商排行如图3-6所示：



△图3-6 2025年中在野利用漏洞数量厂商排行

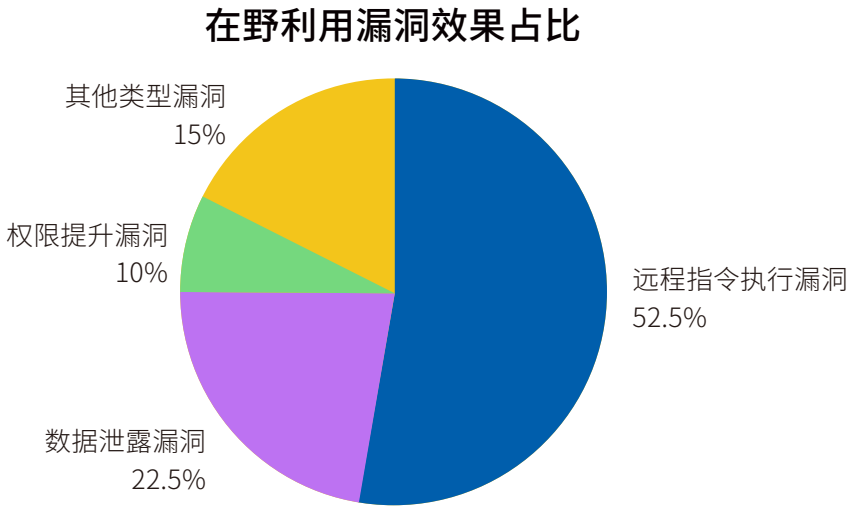
对这些现实利用的漏洞做进一步分析，得到以下结论：

远程漏洞占比89.5%，本地漏洞仅占10.5%，在野利用漏洞威胁类型占比如图3-7所示：



△图3-7 在野利用漏洞威胁远程/本地类型分布

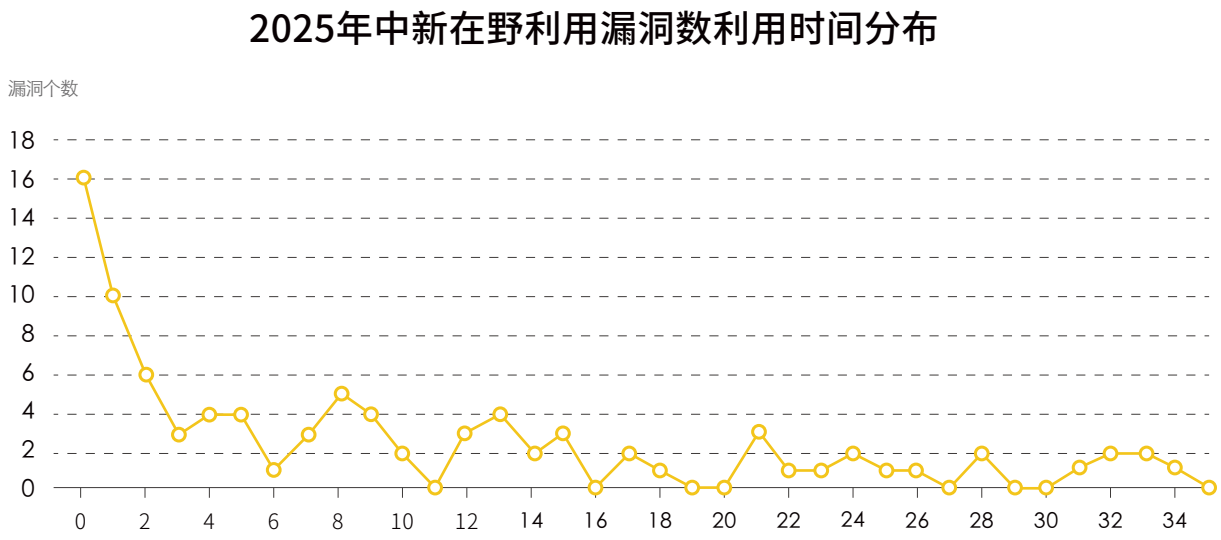
在2025上半年已知被利用的这些漏洞中，能够实现远程指令执行的漏洞或组合漏洞占比52.5%，比例过半，这类漏洞通常危害极高，可以被用来完全控制受影响的系统；数据泄露类型漏洞占比22.5%，这类漏洞以窃取敏感信息为主；权限提升类漏洞多为本地漏洞，占比10.0%，攻击者利用这些漏洞可以在受影响的系统中获取更高的权限。在野利用漏洞威胁类型分布占比如图3-8所示：



△图3-8 在野利用漏洞威胁类型分布

2025上半年已知被利用的漏洞，漏洞信息公开与首次发现在野利用平均时间差值为16天，这比2024年的平均时间差2天还要短，有30.2%的高危漏洞在发布当天就被利用。显示有直接利益驱动的攻击者在持续迭代自己的能力，意味着攻击者持续监控安全公告和漏洞数据库，以便在漏洞公开后立即采取行动，他们对新漏洞的快速识别和利用能力一直在增强。

83.7%的高危漏洞在发布后21天内被利用，所以3周是漏洞的处置黄金时段，组织必须迅速采取行动，以防止这些漏洞被恶意利用。在野利用漏洞平均利用时间如图3-9所示：



△图3-9 2025年中新在野利用漏洞数利用时间分布

部分重要典型新在野利用漏洞分析：

1、vBulletin 远程代码执行漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-48827	万级	代码执行	10.0	是	已公开	已公开	已发现

vBulletin 是最广泛使用的基于 PHP/MySQL 的商业论坛平台之一，为全球数千个在线社区提供支持。黑客曾利用该平台的严重漏洞入侵热门论坛并窃取大量用户的敏感数据。

2025年5月23日，某博客发布vBulletin 远程代码执行漏洞(CVE-2025-48827)文章和技术细节，攻击者可通过模板引擎处理错误从而利用replaceAdTemplate方法实现远程代码执行。随后Dewhurst观测到大量的攻击尝试和利用。但官方已于去年4月份修复该漏洞。

2、Apple iOS/iPadOS 内存破坏漏洞

iOS是由苹果公司开发的移动操作系统。iPadOS是苹果公司基于iOS研发的移动端操作系统系列。iPadOS主要运用于iPad等设备，聚焦了Apple Pencil、分屏和多任务互动功能，并可与Mac进行任务分享。

2025年4月16日，苹果公司发布紧急安全更新，以修补两个零日漏洞。苹果指出，这些漏洞可能已被利用来针对 iOS 上的特定目标用户进行极其复杂的攻击。

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-31200	千万级	代码执行	6.8	否	未公开	未公开	已发现
CVE-2025-31201		代码执行	7.5	否	未公开	未公开	已发现

CVE-2025-31200：iOS 的 CoreAudio 组件中存在内存损坏漏洞。攻击者可能通过处理恶意制作的媒体文件中的音频流来利用此漏洞执行远程代码执行。
CVE-2025-31201：具有任意读写权限的攻击者可以利用此漏洞绕过指针身份验证 (Pointer Authentication)。

3、Ivanti 多款产品缓冲区溢出漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-0282	十万级	代码执行	9.0	否	已公开	已公开	已发现

Ivanti Connect Secure，以前称为Pulse Connect Secure，是一款提供SSL VPN解决方案的产品。它允许远程用户通过一个安全的通道访问企业资源，确保数据在传输过程中的加密和安全。Ivanti Connect Secure是由Pulse Secure公司开发的，该公司后来被Ivanti收购，因此产品名称发生了变化。Ivanti Policy Secure则是一个网络访问控制 (NAC) 解决方案。Ivanti Neurons for ZTA gateways是用于实现零信任访问的网关设备，通过动态验证和授权来保护网络资产。
2025年1月8日，Ivanti 官方修复Ivanti 多款产品缓冲区溢出漏洞(CVE-2025-0282)，Ivanti Connect Secure、Ivanti Policy Secure 和 Ivanti Neurons for ZTA 网关中存在一个基于堆栈的缓冲区溢出漏洞，未经身份验证的远程攻击者可以在易受攻击的设备上实现远程代码执行，官方已确认该漏洞存在在野利用。

4、Fortinet FortiOS 和 FortiProxy 身份认证绕过漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
QVD-2025-13936	百万级	代码执行	8.1	否	未公开	未公开	已发现

Fortinet FortiOS 是美国飞塔（Fortinet）公司的一套专用于FortiGate网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web内容过滤和反垃圾邮件等多种安全功能。FortiProxy 是 Fortinet 推出的一款高性能的安全 Web 网关产品，结合了 Web 过滤、DNS 过滤、数据泄露防护（DLP）、反病毒、入侵防御和高级威胁保护等多种检测技术，以保护用户免受网络攻击。

2025年1月14日，Fortinet 官方修复Fortinet FortiOS 和 FortiProxy 身份认证绕过漏洞(CVE-2024-55591)，FortiOS 和 FortiProxy 中存在一个身份认证绕过漏洞。未经身份验证的远程攻击者可以通过向 Node.js websocket 模块发送特制请求，成功利用此漏洞可使攻击者获得超级管理员权限，官方已确认该漏洞存在在野利用。

5、Palo Alto Networks PAN-OS 身份验证绕过漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-0108	万级	身份认证绕过	8.2	是	已公开	已公开	已发现

PAN-OS 是运行 Palo Alto Networks 下一代防火墙的软件。通过利用 PAN-OS 本机内置的关键技术（App-ID、Content-ID、设备 ID 和用户 ID），可以在任何时间、任何地点完全了解和控制所有用户和设备中正在使用的应用程序。

2025年2月13日，官方修复Palo Alto Networks PAN-OS 身份验证绕过漏洞(CVE-2025-0108)，该漏洞是由于PAN-OS中Nginx/Apache对路径的处理不同导致的。未经授权的攻击者可以利用这一漏洞绕过系统身份验证直接访问Web界面从而造成敏感数据泄露或系统被接管等更大的危害。

2025年 3月11日，The Hacker News 报道称，Palo Alto Networks 确认 CVE-2025-0108 正在被积极利用，攻击者试图将该漏洞与其他漏洞（如 CVE-2024-9474 和 CVE-2025-0111）结合，以获得未修补且未受保护的 PAN-OS 网页管理界面的 root 级别访问权限。

四、APT及勒索软件漏洞

1、APT（高级持续性威胁）攻击事件一直频繁发生，这些攻击通常由国家支持的黑客组织发起，目的是窃取敏感数据、知识产权或进行破坏性活动。

上半年APT攻击态势：

攻击手段多元化：APT组织将 Deepfakes 纳入攻击手段，通过模仿关键人物的声音或制作假视频来欺骗目标，获取敏感信息。同时，BYOVD 技术在 APT 攻击中崛起，攻击者利用驱动程序中的漏洞提升权限、突破安全防御。

开源项目供应链攻击攀升：开源压缩工具 XZ 后门事件凸显了开源生态系统在安全防护上的脆弱性，许多关键开源项目由少数开发人员维护，难以有效抵御复杂的 APT 攻击。

地缘政治影响下的攻击目标明确：如台 APT 组织长期针对我国家政府和公共服务机构等实施网络间谍活动，窃取并向境外反华势力出卖国家重要信息。

2、勒索软件攻击活动目前已经成为对政企机构威胁最大的恶意网络攻击活动，可能直接导致业务的中断和数据的泄露，影响企业经营造成声誉损失。漏洞利用是勒索软件团伙获取目标机构访问权的常用手段。

上半年勒索软件攻击态势：

攻击规模与产业化：勒索软件攻击呈现产业化、专业化发展趋势，新型勒索软件和变种不断涌现，如2025年5月全球新增 J、Datacarry、Worldleaks 等多个双重勒索软件家族。

攻击手法升级：“双重勒索”成为主流攻击手法，攻击者不仅加密受害者文件，还以泄露敏感数据为要挟实施二次勒索。同时，勒索软件常利用边界设备漏洞作为攻击切入点，如 Ivanti Connect Secure VPN、思科 ASA 防火墙等设备的漏洞被用于部署勒索软件。

传播方式多样化：除漏洞利用外，勒索软件还通过其他恶意软件或合法远程管理工具传播，如 Phorpiex 和 P2Pinfect 僵尸网络被用于部署勒索软件，一些勒索软件还会伪装成破解工具类软件进行分发手段。

1、Foxmail for Windows 远程代码执行漏洞

2025年4月10日，奇安信威胁情报中心的红雨滴团队发现 APT-Q-12 组织利用 Foxmail 客户端的高危漏洞（QVD-2025-13936）对国内企业用户发起攻击。情报中心第一时间复现确认了所发现的新漏洞，并将其上报给腾讯 Foxmail 业务团队。

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
QVD-2025-13936	百万级	代码执行	8.1	否	未公开	未公开	已发现

Windows 版 foxmail 存在高危远程代码执行漏洞，影响7.2.25.331版本，攻击者可借助恶意页面或文件在当前进程上下文中执行任意代码，威胁用户终端安全。

2、SAP NetWeaver 任意文件上传漏洞

2025年4月22日，ReliaQuest 发现攻击并报告 SAP，确认漏洞被主动利用。

2025年4月24日，SAP在4月安全补丁日发布修复补丁(SAP Note 3596125)以修复该漏洞，该漏洞被正式披露。

2025年4月29日，针对/developmentserver/metadatauploader端点的扫描激增，37个IP参与扫描，14个IP尝试部署 Web Shell。

2025年4月30日，美国 CISA 将该漏洞列入已知遭利用漏洞（KEV）目录，要求联邦机构于5月20日前完成修复。

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-31324	百万级	代码执行	8.1	否	未公开	未公开	已发现

SAP NetWeaver Visual Composer MetadataUploader 存在未受保护的漏洞，未对上传操作进行适当的授权验证，允许未认证的攻击者上传潜在恶意的可执行二进制文件。攻击者可以利用该漏洞，通过向 /development server/metadatauploader 终端发送恶意 POST 请求，上传 JSP 网络外壳（如 helper.jsp 和 cache.jsp），这些文件会被放置在 j2ee/cluster/apps/sap.com/irj/servletjsp/irj/root/ 目录下，并可通过简单的 GET 请求远程执行。

五、国产软件相关漏洞

2025年上半年，随着数字化转型的加速和国产软件的广泛应用，国产软件漏洞数量呈现出一定的上升趋势。越来越多的国产软件被部署和使用，相应地，其面临的网络安全风险也随之增加，攻击者对国产软件的关注度提高，导致发现并曝光的漏洞数量增多。

国产软件在政府、金融、能源、交通等关键行业以及企业办公自动化等领域有着广泛的应用。一旦这些软件存在漏洞并被利用，可能会导致系统瘫痪、数据泄露、敏感信息被窃取等严重后果，对国家关键基础设施安全、企业商业利益和用户个人信息保护等产生重大影响。

国产软件厂商对安全问题的重视程度需要不断提高，及时发布补丁和修复方案，是缩短漏洞从发现到修复的周期最有效的方法。

1、泛微E-cology9 SQL注入漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
QVD-2025-15550	万级	代码执行	9.8	否	未公开	未公开	未发现
QVD-2025-23834		代码执行	9.8	是	已公开	未公开	未发现

2025年上半年，奇安信CERT监测到泛微E-cology9一共存在两个公开SQL漏洞，分别影响v10.74和v10.75之前的版本。未经身份认证的远程攻击者可利用该漏洞获取数据库敏感信息，并可能利用Ole组件导出为Webshell实现远程代码执行，进而获取服务器权限。

2、契约锁电子签章系统远程代码执行漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
QVD-2025-23408	万级	安全特性绕过代码执行	9.8	是	已公开	已公开	未发现

契约锁是一个电子签章及印章管控平台，提供的电子文件具有与纸质文件一样的法律效力。
2025年6月11日，奇安信CERT监测到契约锁官方修复某处安全漏洞。该漏洞源于管理控制台存在未授权JDBC注入漏洞，攻击者通过构造恶意数据库连接参数，在dbtest接口触发远程代码执行。

3、DataEase 远程代码执行漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-49001	万级	身份验证绕过	9.1	否	未公开	未公开	未发现
CVE-2025-49002		代码执行	8.8	是	已公开	未公开	未发现

DataEase 是一款开源的数据分析平台，提供丰富的数据可视化和分析功能，帮助用户轻松地进行数据探索和决策支持。
2025年6月5日，奇安信CERT监测到DataEase 远程代码执行漏洞POC公开。CVE-2025-49001是由于JWT校验机制错误导致攻击者可伪造JWT令牌绕过身份验证流程，CVE-2025-49002是由于H2数据库模块没有严格过滤用户输入的JDBC连接参数，可使用大小写绕过补丁。攻击者可利用这些漏洞实现未授权代码执行，威胁用户数据和系统的安全。

六、其它类别关键漏洞

1、Apache Kafka Connect任意文件读取漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-27817	万级	信息泄露	7.5	是	已公开	已公开	未发现

Apache Kafka 是一款开源的分布式事件流平台，广泛用于高性能数据管道、流式分析和数据集成。它支持高吞吐量的消息传递，具备可扩展性、持久化存储和高可用性等特点，能够处理海量数据并支持多种编程语言的客户端库。

2025年6月11日，奇安信CERT监测到官方修复了Apache Kafka Connect任意文件读取漏洞。Apache Kafka客户端在处理 SASL/OAUTHBEARER 连接配置时，允许通过配置项指定外部 URL 或本地文件路径。攻击者可以利用该漏洞读取服务器上的任意文件内容，并将其返回到错误日志中。

2、Roundcube Webmail 后台代码执行漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-49113	百万级	代码执行	9.9	是	已公开	已公开	未知

Roundcube Webmail 是一款基于浏览器的多语言 IMAP 客户端，拥有类似应用程序的用户界面。Roundcube 与cPanel 和 Plesk等主流主机控制面板的广泛集成，大大扩大了攻击面。

2025年6月2日，官方发布补丁修复一个存在代码库10年之久漏洞，随后相关POC在论坛上出售，2025年6月6日，相关细节和POC公开。

该漏洞是由于Roundcube Webmail的自定义反序列化函数在处理包含特定分隔符时存在逻辑错误，允许认证攻击者通过构造恶意文件名触发反序列化，最终实现远程命令执行从而完全接管服务器。

3、Elastic Kibana 原型污染致任意代码执行漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-25015	十万级	代码执行	9.9	否	未公开	未公开	未发现
CVE-2025-25014		代码执行	9.1	否	未公开	未公开	未发现

2025年上半年，奇安信CERT监测到Elastic Kibana两个较为严重的原型污染致任意代码执行漏洞(CVE-2025-25015、CVE-2025-25014)。具有特定权限的攻击者通过构造恶意文件上传和特制 HTTP 请求，污染 JavaScript 对象原型链，绕过验证机制执行任意代码。

4、Ivanti Endpoint Manager 信息泄露漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2024-13159	万级	信息泄露	9.8	是	已公开	未公开	已发现

Ivanti Endpoint Manager（EPM）是由Ivanti公司开发的一款综合性端点管理解决方案，它帮助企业有效管理和保护网络中的端点设备，包括桌面、笔记本电脑、服务器、移动设备和虚拟环境等。

2025年1月13日，Ivanti发布补丁修复了Ivanti Endpoint Manager 信息泄露漏洞(CVE-2024-13159)，在 Ivanti EPM 的代理门户中，存在多个绝对路径遍历漏洞。这些漏洞允许远程未经身份验证的攻击者泄露敏感信息。

2025年 3月11日，美国网络安全和基础设施安全局 (CISA) 将该漏洞添加到其已知被利用漏洞 (KEV) 列表中，暂未发现该漏洞被武器化利用。

5、Apache OFBiz 服务端模板注入漏洞

漏洞编号	影响量级	威胁类型	CVSS评分	漏洞威胁状态			
				细节是否公开	PoC状态	EXP状态	在野利用
CVE-2025-26865	万级	信息泄露	9.8	否	未公开	未公开	未发现

Apache OFBiz是一个著名的电子商务平台，提供了创建基于最新 J2EE/ XML规范和技术标准，构建大中型企业级、跨平台、跨数据库、跨应用服务器的多层、分布式电子商务类WEB应用系统的框架。

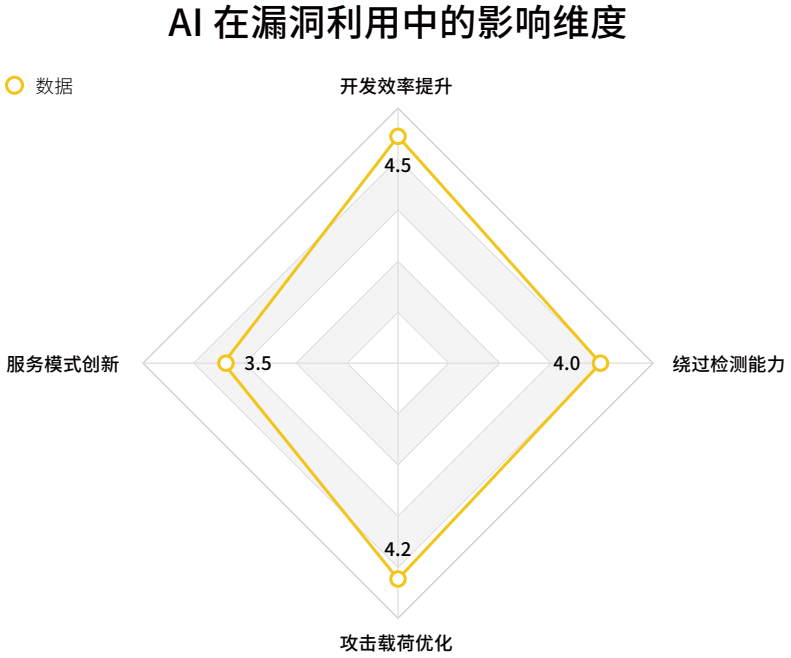
2025年3月7日，Apache官方修复Apache OFBiz 服务端模板注入漏洞(CVE-2025-26865)，Apache OFBiz 存在服务器端模板注入漏洞。攻击者可利用该漏洞，通过精心构造的输入注入恶意模板代码，从而在服务器端执行任意代码，可能导致敏感信息泄露、数据篡改或系统完全被控制。

04

第四章

2025年下半年漏洞新兴技术发展趋势展望

一、AI驱动的漏洞挖掘与利用：攻防智能化升级



△图4-2 AI在漏洞利用中的影响维度

雷达图4-2直观地展示了 AI 技术在漏洞利用的各个维度上所带来的显著影响，预示着未来攻击将更加智能化和高效化。并引出了AI在下半年所遇到的棘手问题：

1.AI漏洞挖掘规模化

自动化审计突破：多智能体系统（如Argusee）通过模拟安全团队协作，可高效定位Linux内核、云原生组件中的0day漏洞（如CVE-2025-37891），漏洞发现效率提升3-5倍。

攻击路径优化：攻击者利用AI生成对抗样本绕过检测（如篡改恶意代码特征），并借助LLM自动混淆攻击载荷，使漏洞利用更隐蔽。

2.AI自身成为新攻击面

本地化部署的AI框架（如Ollama）暴露未授权访问风险，模型权重和训练数据可能被窃取；

恶意提示词注入可触发远程代码执行（如Meta Llama框架漏洞）。

防御建议：部署AI专用漏洞扫描工具（如FUTURE方法），实施提示词过滤与输出审查；隔离训练与生产环境。

二、量子计算冲击传统密码：迁移迫在眉睫

1.威胁实质化

Shor算法可破解RSA/ECC加密，SIM卡、VPN和数字证书体系面临失效风险。中移智库指出，量子计算机可能在未来5年内突破临界点。

2.迁移加速

中国电信已部署全球首个 QKD+PQC融合密码体系，实现千公里级量子加密通信；

金融、政务等高敏系统优先启动抗量子算法（如CRYSTALS-Kyber）试点。

挑战：抗量子算法密钥长度增加（256位以上），导致SIM卡等资源受限设备通信延迟上升。

三、云原生与虚拟化漏洞：架构缺陷引爆风险

1.Kubernetes配置漏洞常态化

IngressNightmare系列漏洞（如CVE-2025-24514）暴露准入控制器设计缺陷，攻击者可通过恶意AdmissionReview请求接管集群，影响43%云环境。

漏洞根因在于：控制面与数据面未分离，导致Nginx配置注入和动态库加载被滥用。

2.无服务器与容器逃逸加剧

函数注入、Kubernetes RBAC配置错误引发横向移动，预计容器逃逸事件下半年增长50%。

防御建议：采用服务网格mTLS加密、容器镜像签名验证；隔离Ingress控制器网络并限制AdmissionReview访问源。

四、物联网设备漏洞：僵尸网络驱动大规模攻击

1.固件漏洞利用产业化

攻击链：弱口令/协议漏洞（如Telnet）→ 植入轻量级RAT（如NOIRWorm、MiraiX）→ 组建百万级僵尸网络（DDoS峰值超5Tbps）。

医疗设备（输液泵）、智能电表成重灾区，因固件更新困难导致漏洞生命周期延长。

2.通信协议暴露

Modbus TCP等OT协议遭大规模扫描，每秒监测36,000次探测请求。

应对措施：强制禁用默认凭证，部署终端行为监控（如检测异常WebSocket连接）

五、漏洞利用产业化：暗网经济助推攻击规模化

1.漏洞即服务（EaaS）成熟

暗网交易零日漏洞（如ATM漏洞标价200万美元），初始访问代理售卖RDP权限（19%）、WebShell（12%）。

2.复合攻击链标准化

典型链：边缘设备漏洞 → 横向移动 → 勒索软件部署，耗时从周缩短至小时。

3.修复窗口消失

28.3%漏洞在披露24小时内遭利用，传统修补机制失效。

六、新兴威胁：供应链与AI泄露风险

1.开源供应链漏洞激增

开发密钥泄露（如GitLab令牌占50%）平均94天才修复，攻击者通过SBOM信息精准打击依赖库。

2.AI数据泄露

15%员工向ChatGPT上传未脱敏文档，生成式AI成敏感数据外泄新渠道。

七、防御体系构建与策略建议

1.技术层防御框架

EPSS与KEV融合模型：提升修复效率40%，动态调整优先级。

AI漏洞扫描：部署工具（如奇安信天擎），结合白名单与快照。

网络隔离：实施微隔离，限制横向移动。

2.管理流程优化

漏洞管理委员会：由CISO牵头，定期评审。

自动化响应流水线：对接ITSM系统，实现闭环管理。

红蓝对抗演练：每季度模拟零日攻击。

05

第五章

漏洞处置建议

全面漏洞管理体系建设：

企业应采用先进的漏洞扫描工具和补丁管理系统，并定期进行安全评估。

加强漏洞治理能力：

部署自动化漏洞扫描和修复工具，缩短漏洞修复时间。针对高危漏洞优先修复，并加强关键业务系统的隔离保护。

应对新兴威胁：

部署量子抗性算法，逐步升级现有加密协议。对云原生架构和物联网设备进行持续安全审计，防范新兴攻击面。

强化供应链安全：

对开源组件和第三方服务供应商进行安全评估，确保供应链透明性和安全性。

提升安全意识与技能：

定期开展员工网络安全培训，提升全员对社会工程和安全威胁的应对能力。

推广零信任架构：

进一步部署零信任安全架构，从身份验证、访问控制到数据保护全方位抵御漏洞利用。

最新风险通知：

奇安信漏洞订阅服务可以帮助你从互联网海量的漏洞信息里筛选出真正有价值的那一部分，及时获得与组织相关的安全漏洞情报。

06

第六章

总结

2025年上半年，漏洞态势呈现**风险集中化、攻击智能化、防御体系化特征。**KEV漏洞占0.38%，覆盖82%高风险场景。企业需通过**数据驱动、智能决策、协同防御**，从被动修复转向主动防御，以应对日益复杂的漏洞威胁环境。

07

第七章

奇安信漏洞情报服务订阅

根据奇安信安全监测与响应中心大数据统计，每年监测到的漏洞信息高达数万条，平均每天新增上百条。如果依靠企业自身的安全部门处理这些漏洞势必会投入相当多的资源和成本，并且也容易遗漏一些不起眼却又危害极大的漏洞。面对井喷式的漏洞信息增长，传统“条文式”漏洞修补和防护的管理模式，已经无法适应数字化转型深入的要求，需要依靠外部可靠的漏洞情报对企业安全生产进行支持与管理。漏洞的处理从人工转向自动化成为必然趋势，企业安全能力体系及安全运行体系的升级，需要更加先进的漏洞情报体系进行支撑。

奇安信漏洞订阅服务可以帮助你从互联网海量的漏洞信息里筛选出真正有价值的那一部分，及时获得与组织相关的安全漏洞情报，同时为您提供可行的包含详细操作步骤的处置措施。这种服务会向您提供实时更新的、富化的漏洞信息报告，包括最新发现的漏洞、已知的漏洞和修补程序的建议。您可以根据报告中的内容迅速定位和排查自己的资产风险，及时采取有效的防范措施，更加高效的进行企业漏洞管理。奇安信漏洞情报服务具有如下优势：

一、最全面、最值得信赖的漏洞库

收录1999年以来全量38万余条漏洞信息，涵盖通用网络产品漏洞、工业控制漏洞、信创政务漏洞、车联网漏洞等多个领域。开源漏洞信息覆盖率达到100%，自研漏洞信息占比大于20%，核心信息完整率达到99%。

二、高效的漏洞情报运营

分析团队依据完善的流程和专业经验，对漏洞的影响面和技术细节进行研判，把真正重要的漏洞过滤出来，对关键漏洞进行重点运营和持续跟踪，保证信息的准确性、及时性和处理优先级的可靠性。

三、及时的漏洞风险通知

关键漏洞信息2小时内完成研判、定级和入库，保证用户能够第一时间查询获取。发生重大漏洞事件时，能够快速准确地识别、分析、定位漏洞，及时通过邮件、IM、API接口等方式将漏洞风险通知到客户，并给出可靠的缓解措施和修复方案。

四、提供技术细节深入分析与验证

针对影响面巨大、威胁等级极高的漏洞提供独家深度分析报告，对漏洞进行深入分析和技术验证，披露漏洞技术细节、复现测试方法，基于漏洞深度分析提供更加详尽的处置步骤和自查检测方案。

五、灵活的API数据接口

对外输出形式，不仅提供基于多维属性筛选的Web访问界面，还提供在线数据获取的API接口及离线数据包，用户可以根据自己需要集成到自有漏洞处理流程。

六、定制化漏洞应急响应服务

支持基于厂商和软件名的推送订阅，可结合本地安全资产库，通过组件版本自动匹配受影响的资产，实现企业资产关联漏洞预警。提供定制化漏洞深度分析报告解答和技术咨询。

点击订阅（超链接：https://ti.qianxin.com/portal/subscription）

奇安信 | 奇安信 威胁情报中心

邮箱：ti_support@qianxin.com
电话：95015
官网：https://ti.qianxin.com
扫描关注我们的微信公众号