奇安信
威胁情报中心

2024年度
网络安全漏洞威胁态势研究报告

2025年1月

前言 Preface

2024年，全球网络安全领域继续面对日益严峻的挑战。在数字化转型的大背景下，漏洞利用成为网络攻击的重中之重。根据统计，全球新增漏洞数量再创新高，漏洞的复杂性加剧，修复周期也在不断缩短。然而，攻击者的手段日趋复杂，基于漏洞的攻击路径更加隐蔽且复合化。开源项目、云计算、物联网（IoT）、国产软件以及关键基础设施领域漏洞威胁显著增加。

展望2025年，人工智能、量子计算、云原生架构和物联网的快速发展进一步扩展了漏洞暴露面。漏洞挖掘、修复和利用的矛盾将成为未来的攻防焦点。本报告立足2024年奇安信CERT汇集的漏洞数据、典型案例及安全事件，全面展示漏洞态势，同时也对2025年漏洞相关新兴技术发展趋势作出前瞻性展望，为企业、政府机构和网络安全从业者提供参考。

摘要 summary

2024年漏洞态势的关键发现：

漏洞数量持续增长：2024年新增漏洞43,757个，同比增长46.7%，其中高危漏洞占比17.8%，总体漏洞威胁程度持续加深。

漏洞从暴露到被利用时间窗口持续缩短，平均时间18天，对有实际威胁的漏洞识别与及时修补提出了越来越大的挑战。

漏洞深度助力APT攻击：APT组织更倾向于使用零日漏洞和复合攻击链，目标集中于政府、能源、金融及国产软件行业。

国产软件漏洞更多关注：706个国产软件漏洞被披露，主要集中于OA、ERP等，暴露国内软件安全审计能力不足。

供应链来源漏洞显示高威胁度：供应链漏洞频发，典型案例如XZ　Utils工具库后门事件，其传播范围广泛、修复难度大。

勒索软件持续通过漏洞攻击获益：勒索软件团伙频繁利用漏洞进行攻击，高危行业为医疗、教育和能源领域。

2025年漏洞发展趋势展望：

AI驱动的漏洞挖掘与利用：人工智能将被广泛用于漏洞发现、分析和攻击路径优化，攻击及防御复杂性大幅度提升。

量子计算冲击传统密码算法：量子计算能力逐步突破，对传统加密协议可能在远期产生影响。

云原生与虚拟化漏洞爆发：云原生架构中的容器逃逸、Kubernetes配置错误等漏洞成为热点。

物联网设备漏洞激增：物联网设备固件漏洞和通信协议漏洞被攻击者大规模利用。

漏洞利用自动化与产业化：漏洞利用即服务（Exploitation-as-a-Service）将推动漏洞攻击规模化。

目录 Table of contents

目录 Table of contents

01

2024年度漏洞态势分析

第一章

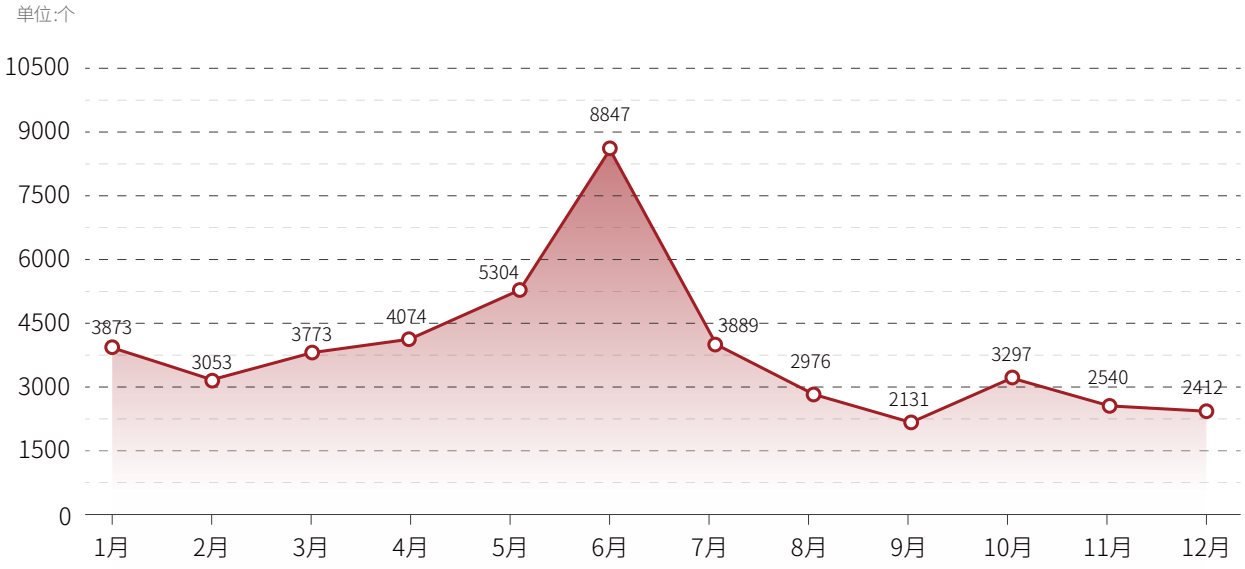
一、漏洞数量统计与趋势

2024年1月1日至12月31日期间，奇安信安全监测与响应中心（又称奇安信CERT）共监测到新增漏洞43757个，较2023年同比增长46.7%。总高危、极危漏洞数量为7777个，占总量的17.8%。**漏洞数量激增的主要原因包括技术生态复杂化、开源组件应用增加以及攻击者专业化程度提升。**

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965个[1]，达到发布安全风险通告标准的漏洞共392个[2]，并对其中82个漏洞进行深度分析[3]。

43757个 奇安信安全监测与响应中心共监测到新增漏洞	**46.7%** 较2023年同比增长	**7777个** 高危漏洞触发了人工研判
965个 本年度值得重点关注的漏洞	**392个** 达到奇安信CERT发布安全风险通告标准的漏洞	**82个** 漏洞进行深度分析

2024年每月新增漏洞数量



△图1-1 2024年奇安信CERT漏洞库每月新增漏洞信息数量

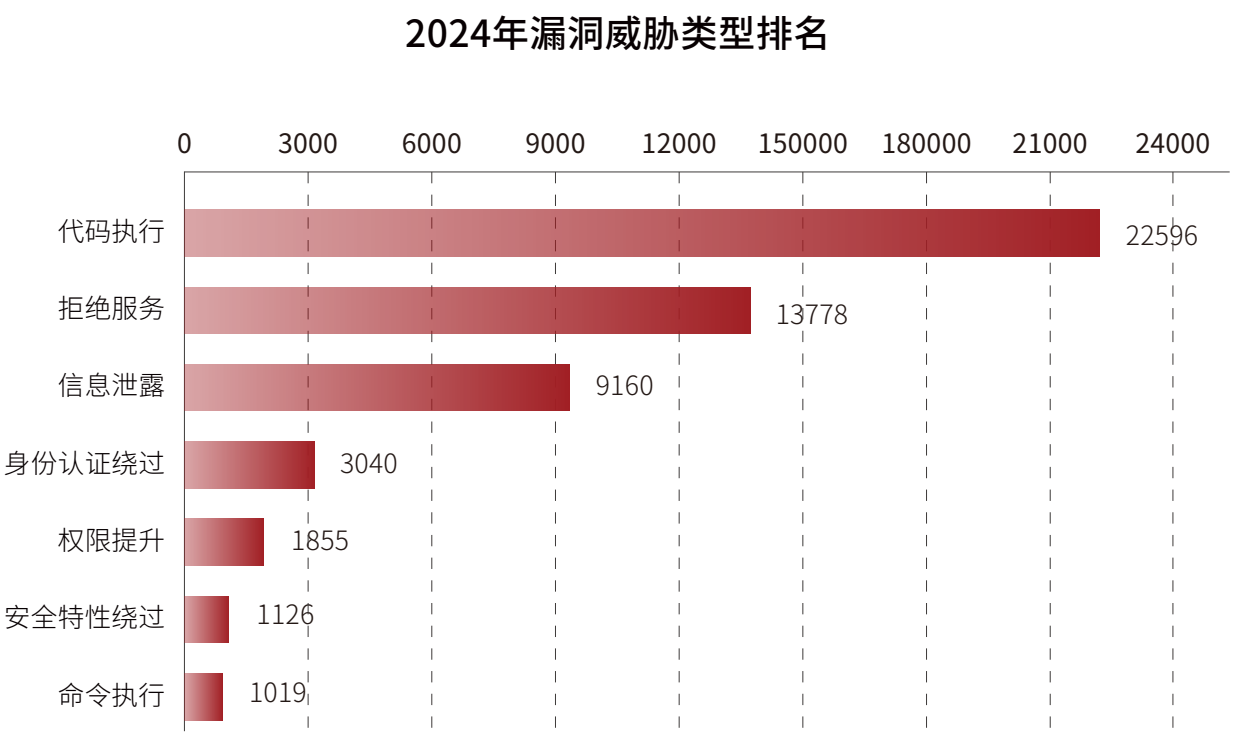
2024年漏洞披露高峰为1月和6月，这与年度安全更新周期和大规模披露活动相关。攻击集中时间在下半年，体现了攻击者利用企业年末漏洞修复滞后的情况。

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

二、漏洞威胁类型占比情况

代码执行、信息泄露和权限提升是攻击者利用的漏洞核心类型，特别是在复杂攻击链中。

对2024年度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、拒绝服务、信息泄露。这些类型的漏洞通常很容易被发现、利用，其中代码执行、权限提升类型的漏洞可以让攻击者完全接管系统、窃取数据或阻止应用程序运行，具有很高的危险性，应该成为安全从业人员的重点关注对象。

三、漏洞影响厂商与行业分布

将2024年度新增的43757个条漏洞信息根据漏洞影响厂商进行分解，如图1-3所示：

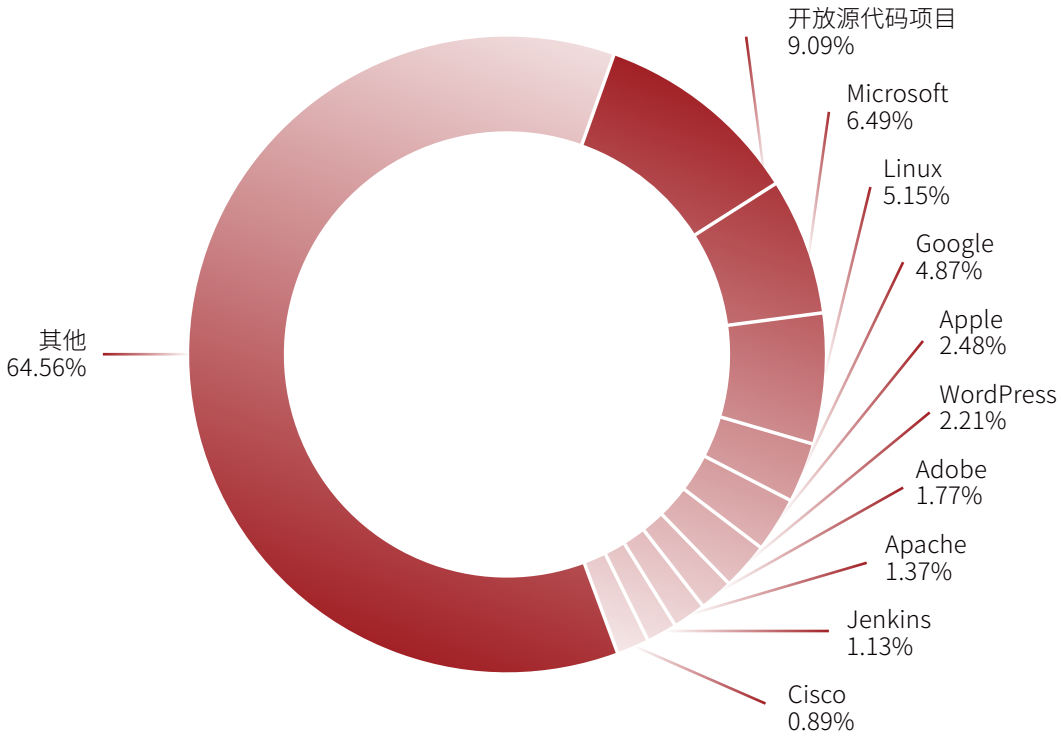
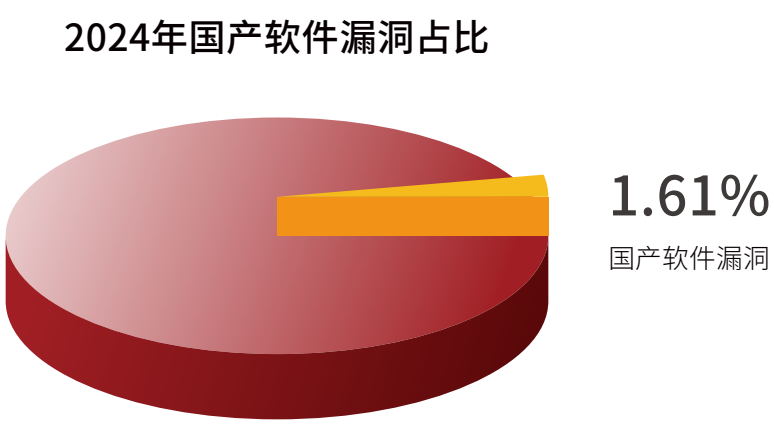


图1-3 漏洞影响厂商占比

其中漏洞数量占比最高的前十家厂商为：开放源代码项目、Microsoft、Linux、Google、Apple、WordPress、Adobe、Apache、Jenkins、Cisco。Google、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。

2024年新增的漏洞中，有706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。这些漏洞中OA和ERP系统尤为突出。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。



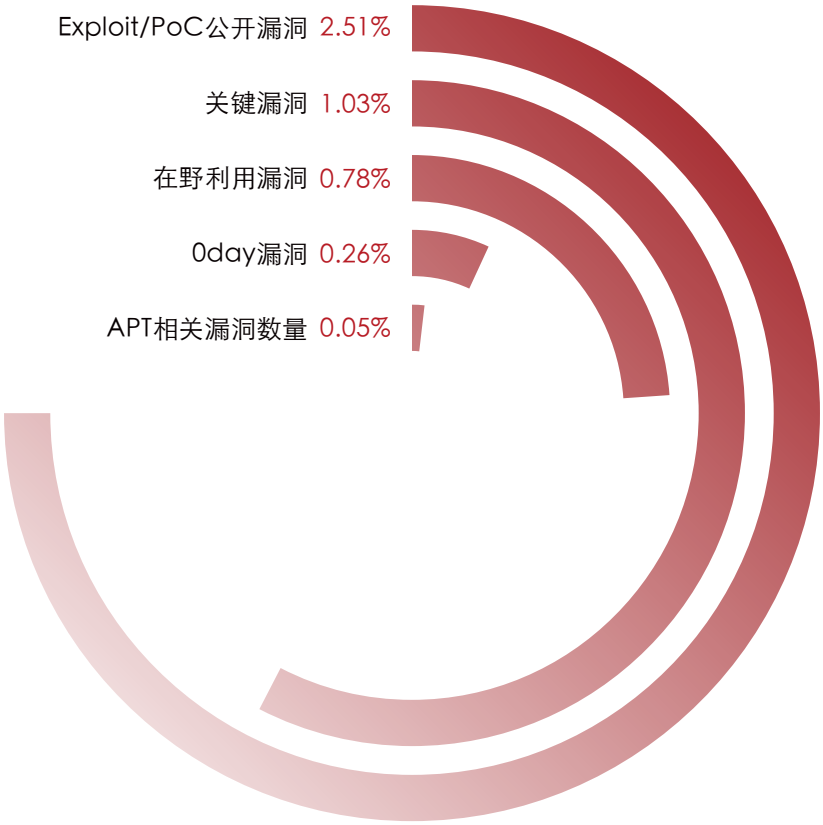
△图1-4 国产软件漏洞占比

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。

2024年奇安信CERT共标记关键漏洞450个，占全年新增漏洞的1.03%；存在公开Exploit/PoC漏洞数量为1100个，占全年新增漏洞的2.51%；发现已有在野利用漏洞数量为343个，占全年新增漏洞的0.78%；0day漏洞数量为113个，占全年新增漏洞的0.26%；APT相关漏洞数量为24个，占全年新增漏洞的0.05%。

上述各类漏洞在2024年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。

△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2024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	OpenSSH 远程代码执行漏洞	CVE-2024-6387	高危	升级至OpenSSH 9.8p1 或更高版本
2	Windows 远程桌面 授权服务远程代码执行漏洞	CVE-2024-38077	高危	安装补丁
3	Windows TCP/IP IPv6 远程拒绝服务/代码执行漏洞	CVE-2024-38063	高危	安装补丁
4	XZ Utils 工具库 恶意后门植入漏洞	CVE-2024-3094	高危	目前官方尚无最新版本，需对软件版本进行降级5.4.X，请关注官方新版本发布并及时更新。
5	Oracle WebLogic Server JNDI 注入漏洞	CVE-2024-20931	高危	安装补丁
6	Internet快捷方式文件 安全特性绕过漏洞	CVE-2024-21412	高危	安装补丁
7	7-Zip 代码执行漏洞	CVE-2024-11477	高危	升级至7-Zip 24.07 或更高版本
8	VMware vCenter Server 多个堆溢出漏洞	CVE-2024-37079 CVE-2024-37080	高危	建议受影响用户升级至最新版本：VMware vCenter Server 8.0 U2d、VMware vCenter Server 8.0 U1e、VMware vCenter Server 7.0 U3r、VMware Cloud Foundation 5.x/4.x KB88287
9	Jenkins Remoting 任意文件读取漏洞	CVE-2024-43044	高危	升级至Jenkins 2.471、LTS 2.452.4、LTS 2.462.1或更高版本
10	Apache Tomcat 拒绝服务漏洞	CVE-2024-34750	高危	升级至Apache Tomcat 9.0.90、10.1.25、11.0.0-M21或更高的版本

在本年度总热度舆论榜前十的漏洞中，热度最高的漏洞为OpenSSH 远程代码执行漏洞(CVE-2024-6387)。该漏洞是由于OpenSSH服务器（sshd）中的信号处理程序竞争问题，未经身份验证的攻击者可以利用此漏洞在Linux系统上以root身份执行任意代码。但是，漏洞的热度高并不一定代表漏洞的实际风险大。该漏洞为之前CVE-2006-5051漏洞修补不完善导致的二次引入，当前的漏洞利用代码仅针对在32位Linux系统上运行的OpenSSH，64位Linux系统上利用该漏洞的难度会更大，在Linux系统上以Glibc编译的OpenSSH上成功利用，不过利用过程复杂、成功率不高且耗时较长。平均要大于10000次才能赢得竞争条件，需要6~8小时才能获得远程root shell。在以非Glibc编译的OpenSSH上利用此漏洞据说也是可能的，但尚未证实。虽然目前还没有发现真正实现远程代码执行的POC，鉴于该漏洞影响范围较大，建议受影响用户升级至OpenSSH 9.8p1。

七、2024年最危险的CWE类型

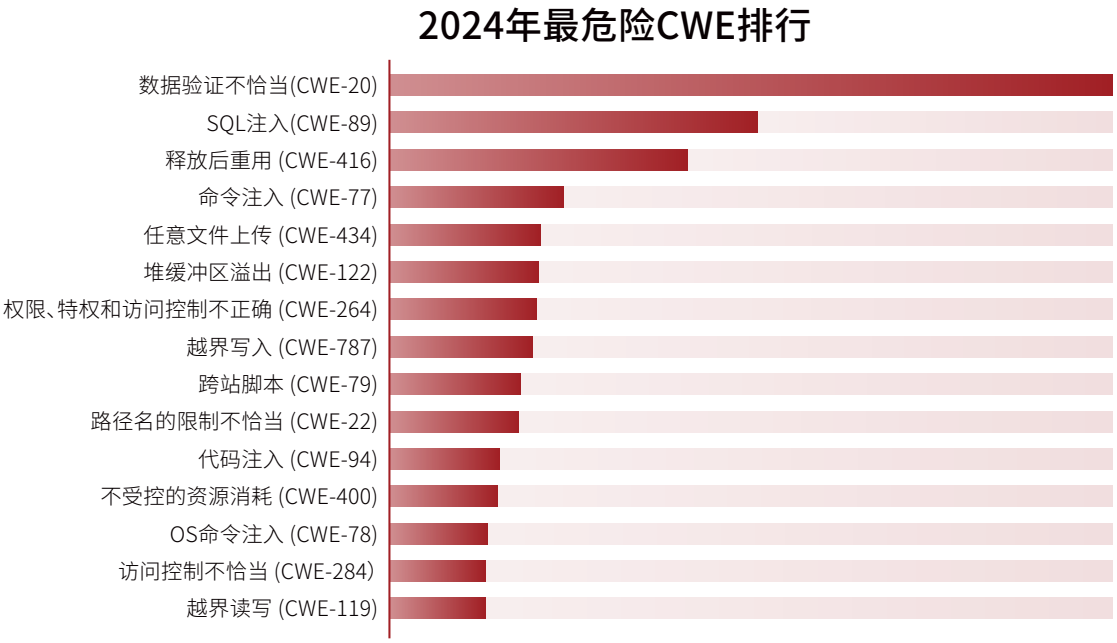
CWE 是代码、设计或架构中可能导致漏洞的常见软件弱点或缺陷的列表，它们本身列在常见漏洞和披露（CVE）数据库中。某些漏洞通常很容易找到并加以利用，攻击者通过这些漏洞能够窃取数据、完全接管系统或阻止应用程序运行。CWE 是这些漏洞的根本原因。

为了定义软件弱点的严重性级别，2024年，奇安信CERT汇集本年度7777个高危、极危漏洞，从中总结出最危险 CWE 列表供参考。2024年最危险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。

今年，在7777个高危、极危漏洞中，数据验证不恰当（也称为“输入验证不恰当“（CWE-20））占据首位，有1201个漏洞，占总数的15.44%。

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）位居第二，有608个漏洞，且存在很多已知被利用的相关漏洞，占总数的7.82%。

第三名是释放后重用（CWE-416），有494个漏洞，占总数的6.35%。

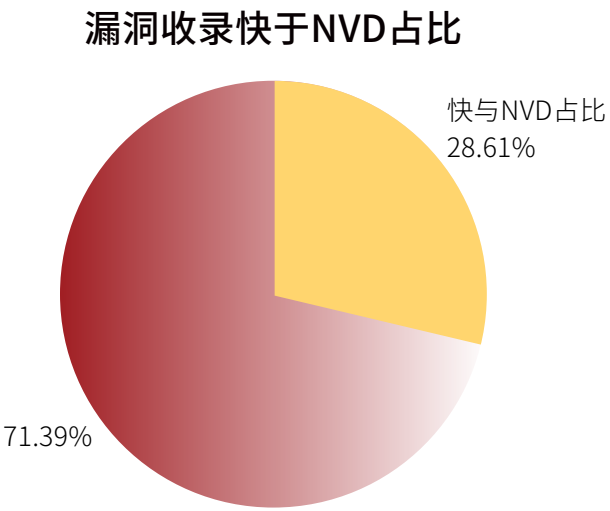


△图1-7 2024年最危险CWE排行

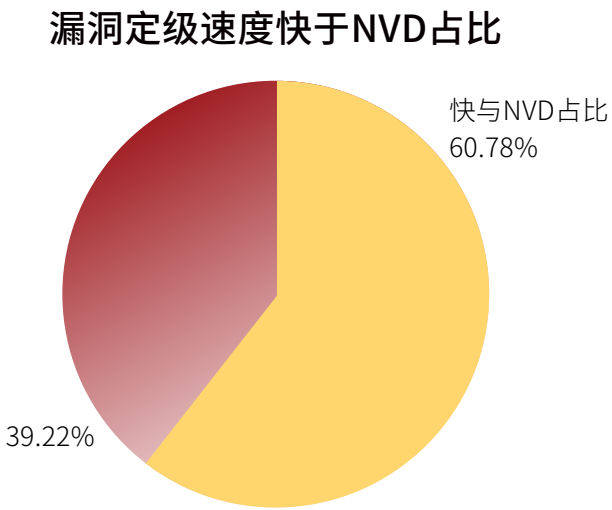
建议查看此列表并通过它获悉软件安全策略。在开发和采购流程中优先考虑这些弱点有助于防止软件生命周期核心的漏洞。

八、漏洞修复时效性

2024年漏洞平均修复时间：45天，较2023年缩短10%。零日漏洞修复不足：75个零日漏洞中30%修复时间超过30天，部分漏洞已在披露前被利用。披露与利用时间差：公开后4天内被利用的漏洞占50%。
值得注意的是，2024年新增中，有33564个漏洞存在CVE编号，其中有9602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28.6%，且漏洞平均定级速度快于NVD约61%。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

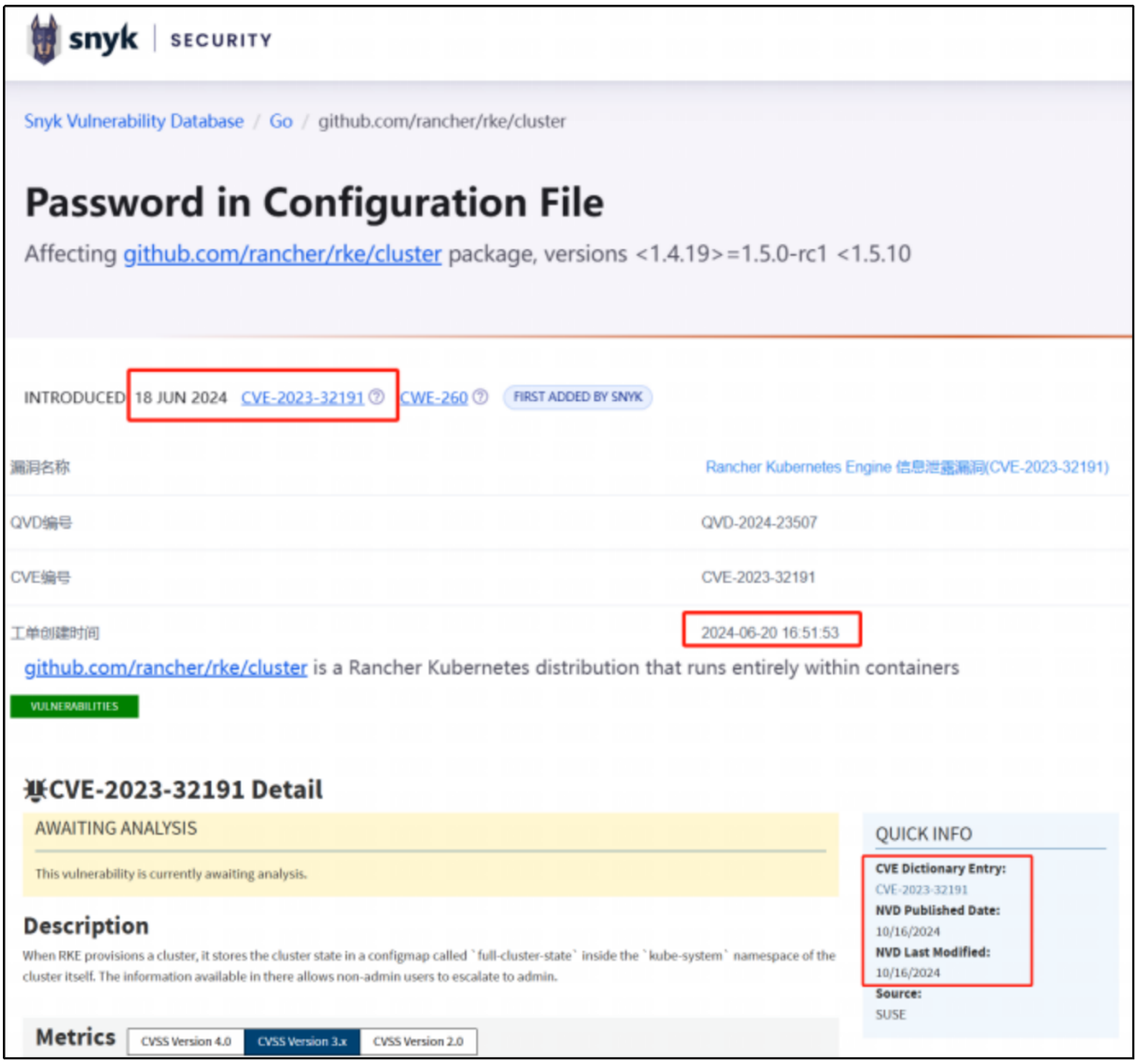


△图1-9 漏洞定级速度快于NVD占比

在这些漏洞中，奇安信CERT漏洞收录时间平均快NVD约6天4小时，其中，Rancher Kubernetes Engine 信息泄露漏洞(CVE-2023-32191)收录时间快NVD约119天，达到本年度之最。奇安信CERT在2024年6月20日捕获漏洞信息源，由分析人员研判入库，而NVD在长达119天后的2024年10月16日公开此漏洞。
漏洞时间线如表1-10所示：

2024年06月11日	Rancher通告Github公开修复漏洞。
2024年06月18日	SNYK率先发布CVE，公开漏洞信息。
2024年06月20日	奇安信CERT捕获到厂商发布CVE，分析人员研判入库。
2024年10月16日	NVD发布并公开CVE信息。

△表1-10 CVE-2023-32191漏洞公开时间线



△图1-10 CVE-2023-32191漏洞公开时间对比图

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

重大漏洞案例分析

第二章

本章节梳理了2024年度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、XZ Utils 库中发现秘密后门，触发紧急安全警报

事件描述

2021年，一个名为”Jia Tan”的人员 创建了 GitHub 账户，之后积极参与 XZ Utils 项目的维护，并逐渐获取信任，最终获得了直接 commit 代码并管理项目的权限。2024年2月，”Jia tan” 向 liblzma/xz 项目中提交恶意文件。2024年3月28日，Ubuntu 注意到一个上游的漏洞影响了 xz-utils 源代码包。2024年3月29日，开发人员 Andres Freund 在安全邮件列表上报告称，他在调查 SSH 性能问题时发现了涉及 XZ 包的供应链攻击，进一步溯源发现 SSH 使用的上游 liblzma 库被植入了后门代码，当满足一定条件时，将会解密流量里的 C2 命令并执行。

关联漏洞

1. XZ Utils 工具库恶意后门植入漏洞(CVE-2024-3094)

受影响版本	xz == 5.6.0　　xz == 5.6.1 liblzma== 5.6.0　　liblzma== 5.6.1
影响量级	万级
危害描述	SSH 使用的上游 liblzma 库被植入了后门代码，当满足一定条件时，将会解密流量里的 C2 命令并执行。
修复措施	建议 XZ Utils 的开发人员和用户降级到已知的、不受影响的 XZ Utils 版本，例如 5.4.6 Stable。除了降级之外，强烈建议开发人员和用户进行事件响应，以确定他们是否受到此后门的影响。

二、黑客利用零日漏洞攻破 Palo Alto Networks 的数千个防火墙

事件描述

2024 年 4 月 10 日，Volexity 在其一家网络安全监控 (NSM) 客户处发现了 Palo Alto Networks PAN-OS 的 GlobalProtect 功能中发现的漏洞的零日利用。Volexity 收到了有关来自客户防火墙的可疑网络流量的警报。随后的调查确定该设备已被入侵。第二天，即 2024 年 4 月 11 日，Volexity 在其另一家 NSM 客户处发现了同一威胁行为体进一步的相同利用。Volexity 使用别名 UTA0218 跟踪的威胁行为体能够远程利用防火墙设备、创建反向 shell 并将更多工具下载到设备上。攻击者专注于从设备导出配置数据，然后利用它作为入口点在受害组织内横向移动。

Palo Alto Networks PSIRT 团队确认该漏洞为操作系统命令注入问题，并将其编号为 CVE-2024-3400。该漏洞是一个无需身份验证的远程代码执行漏洞，CVSS 基本分数为 10.0。此后，Palo Alto Networks 针对 CVE-2024-3400发布了公告，其中包含有关向客户发布的威胁保护签名的信息以及修复时间表，修复时间为 2024 年 4 月 14 日。

关联漏洞

1. Palo Alto Networks PAN-OS 命令注入漏洞(CVE-2024-3400)

受影响版本	PAN-OS 11.1.* < 11.1.2-h3　　PAN-OS 11.0.* < 11.0.4-h1 PAN-OS 10.2.* < 10.2.9-h1
影响量级	十万级
危害描述	未经身份验证的攻击者可能利用此漏洞在防火墙上以root权限执行任意代码。
修复措施	此问题已在 PAN-OS 10.2.9-h1、PAN-OS 11.0.4-h1、PAN-OS 11.1.2-h3 以及所有更高版本的 PAN-OS 版本中修复。

三、零点击 Windows TCP/IP RCE 会影响所有启用 IPv6 的系统，请立即修补

事件描述

微软周二警告客户修补一个严重的 TCP/IP 远程代码执行 (RCE) 漏洞，该漏洞被利用的可能性较高，会影响所有使用 IPv6（默认情况下启用）的 Windows 系统。该安全漏洞由昆仑实验室的研究人员发现，编号为CVE-2024-38063，根因为整数下溢问题，攻击者可以利用该漏洞触发缓冲区溢出，从而可能导致在易受攻击的 Windows 10、Windows 11 和 Windows Server 系统上执行任意代码，但最直接的威胁应该是远程拒绝服务，使目标Windows系统蓝屏重启。

该安全研究员在推特上表示："考虑到其危害，我不会在短期内透露更多细节"，并补充道，在本地 Windows 防火墙上阻止 IPv6 不能阻止漏洞被利用，因为该漏洞在被防火墙处理之前就被触发。未经身份验证的攻击者可以通过反复发送包含特制数据包的 IPv6 数据包，在低复杂度攻击中远程利用此漏洞。由于 CVE-2024-38063 被利用的可能性增加，微软仍建议用户立即应用当月的 Windows 安全更新。

关联漏洞

1. Windows TCP/IP IPv6远程拒绝服务/代码执行漏洞(CVE-2024-38063)

受影响版本	Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-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 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems 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 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems 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	未经身份验证的远程攻击者可以通过反复发送特制的 IPv6 数据包到 Windows 机器上导致目标机器蓝屏崩溃，成功利用此漏洞也存在远程代码执行的可能性导致易受攻击的系统完全攻陷。
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。

四、谷歌披露 Chrome 零日漏洞，已被用于部署恶意软件

事件描述

谷歌修复了今年被标记为利用的第九个 Chrome 零日漏洞，该高危零日漏洞是由 Chrome V8 JavaScript 引擎中的类型混淆缺陷引起的。微软威胁情报中心 (MSTIC) 和微软安全响应中心 (MSRC) 的安全研究人员在2024年8月19日报告了该漏洞。目前已发现黑客利用最近修补的 Google Chrome 零日漏洞 (CVE-2024-7971)，在利用 Windows 内核漏洞获取系统权限后部署 FudModule 根工具包。
此漏洞使黑客能够在重定向到攻击者控制的网站 voyagorclub[.]space 的目标的沙盒 Chromium 渲染器进程中获得远程代码执行。逃离沙盒后，他们使用受感染的 Web 浏览器下载了针对 Windows 内核中的 CVE-2024-38106 漏洞，这使他们获得了 SYSTEM 权限。

关联漏洞

1.Google Chrome V8 类型混淆漏洞(CVE-2024-7971)

受影响版本	Google Chrome(Windows/Mac) < 128.0.6613.84/.85 Google Chrome(Linux) < 128.0.6613.84
影响量级	千万级
危害描述	攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而获取敏感信息或代码执行。
修复措施	手动检查更新： 可通过Chrome 菜单-【帮助】-【关于 Google Chrome】检查版本更新，并在更新完成后重新启动。

五、UNC5820 威胁集群利用 Fortinet 零日漏洞窃取企业配置数据

事件描述

网络安全公司 Fortinet日前披露了自家软件产品 FortiManager 存在的一个关键零日漏洞，能够允许未经身份验证的远程攻击者通过特制请求执行任意代码或命令。目前该漏洞已在野外被积极利用。参与此漏洞调查的Mandiant表示，一个新的威胁组织UNC5820早在2024年6月27日就利用了FortiManager 漏洞，泄露并暂存了FortiManager 管理的 FortiGate 设备配置数据，其中包含受托管设备的详细配置信息以及用户的 FortiOS256 加密密码，这些数据可能被 UNC5820 用来进一步破坏 FortiManager，并在企业环境中横向移动。

根据 Fortinet 10月23日发布的报告，该漏洞被追踪为CVE-2024-47575，CVSS v3 评分高达9.8，对多个版本的 FortiManager 以及 FortiManager Cloud 都有影响。该公司已经发布了一个补丁，并列出了用户可以采用的几种解决方法。

关联漏洞

1. Fortinet FortiManager 身份认证绕过漏洞(CVE-2024-47575)

受影响版本	7.6.0 <= FortiManager 7.6.* <= 7.6.0 7.4.0 <= FortiManager 7.4.* <= 7.4.4 7.2.0 <= FortiManager 7.2.* <= 7.2.7 7.0.0 <= FortiManager 7.0.* <= 7.0.12 6.4.0 <= FortiManager 6.4.* <= 6.4.14 6.2.0 <= FortiManager 6.2.* <= 6.2.12 7.4.1 <= FortiManager Cloud 7.4.* <= 7.4.4 7.2.1 <= FortiManager Cloud 7.2.* <= 7.2.7 7.0.1 <= FortiManager Cloud 7.0.* <= 7.0.12 FortiManager Cloud 6.4.*
影响量级	十万级
危害描述	成功利用漏洞后攻击者将能够查看和修改文件（例如配置文件）以获取敏感信息，并能够管理其他设备执行任意代码或命令。
修复措施	根据您所运行的版本，升级到固定版本或使用以下解决方法之一： 1.对于 FortiManager 版本 7.0.12 或更高版本、7.2.5 或更高版本、7.4.3 或更高版本（但不包括 7.6.0），阻止未知设备尝试注册； 2.对于 FortiManager 7.2.0 及以上版本，可以添加本地策略以将允许连接的 FortiGates 的 IP 地址列入白名单； 3.对于 7.2.2 及以上版本、7.4.0 及以上版本、7.6.0 及以上版本，也可以使用自定义证书来缓解此问题。

六、Firefox 零日漏洞被网络犯罪集团使用

事件描述

Tor 匿名网络上周发布了发布，该漏洞被标记为CVE-2024-9680。该漏洞是由网络安全公司 ESET 的一名研究人员发现的，并由 Mozilla 基金会在其 Firefox 网络浏览器中首次修补。有报告提到，RomCom 网络犯罪集团正在利用CVE-2024-9680与其他漏洞（如CVE-2024-49039）联合进行攻击分发恶意控制软件，目标包括使用Firefox和Tor浏览器的用户。

该漏洞无需用户交互，可通过网络执行，复杂度较低。该漏洞的 CVSS 评分为 9.8（满分 10 分），表明这是一个严重漏洞，为了解决该漏洞，Mozilla 和 Tor 都建议用户将其浏览器安装更新到最新版本。

关联漏洞

1. Mozilla Firefox Animation timelines 释放后重用漏洞(CVE-2024-9680)

受影响版本	Firefox < 131.0.2　Firefox ESR < 128.3.1　Firefox ESR < 115.16.1
影响量级	千万级
危害描述	远程攻击者能够通过利用 Animation timelines 中的释放后使用漏洞在内容进程中实现代码执行。
修复措施	1.用户应避免访问不明网站和点击可疑链接，以减少被攻击的风险。 2.启用浏览器的安全功能，如禁用JavaScript，以降低攻击风险。

七、VMware vCenter Server 中的关键 RCE 漏洞现已被利用于攻击

事件描述

2024年11月20日，Broadcom 警告称，攻击者目前正在利用两个 VMware vCenter Server 漏洞，其中一个是严重的远程代码执行漏洞。

TZL 安全研究人员报告了 RCE 漏洞(CVE-2024-38812)。该漏洞是由 vCenter 的 DCE/RPC 协议实现中的堆溢出问题引发的，影响包含 vCenter 的产品，包括 VMware vSphere 和 VMware Cloud Foundation。另一个存在在野利用的 vCenter Server 漏洞（由同一研究人员报告）是权限提升漏洞，其编号为 CVE-2024-38813，攻击者可以利用该漏洞使用特制的网络数据包将权限提升到 root 权限。

Broadcom 表示："更新公告指出，Broadcom 旗下的 VMware 确认 CVE-2024-38812 和 CVE-2024-38813 已被利用。"

关联漏洞

1. VMware vCenter Server 堆溢出漏洞(CVE-2024-38812)

受影响版本	VMware vCenter Server 8.0 < 8.0 U3b　VMware vCenter Server 7.0 < 7.0 U3s VMware Cloud Foundation 5.x < 8.0 U3b　VMware Cloud Foundation 4.x < 7.0 U3s
影响量级	万级
危害描述	攻击者可能利用此漏洞获取更高权限，进一步控制vCenter Server，执行恶意操作。
修复措施	受影响的用户应立即更新到最新的修复版本。

2. VMware vCenter Server 权限提升漏洞(CVE-2024-38813)

受影响版本	VMware vCenter Server 8.0 < 8.0 U3b　VMware vCenter Server 7.0 < 7.0 U3s VMware Cloud Foundation 5.x < 8.0 U3b　VMware Cloud Foundation 4.x < 7.0 U3s
影响量级	万级
危害描述	攻击者可能利用此漏洞获取更高权限，进一步控制vCenter Server，执行恶意操作。
修复措施	受影响的用户应立即更新到最新的修复版本。

八、微软高危漏洞“狂躁许可”引起广泛关注

事件描述

2024年7月9日，微软官方发布了一个针对Windows 远程桌面授权服务远程代码执行漏洞(CVE-2024-38077) 的修复补丁包，并没有引起大家的警觉。8月在国外某网站上疑似漏洞的作者公开了该漏洞的“POC验证代码”。一时激起千层浪，该漏洞开始疯狂发酵，热度大涨。多年来在 Windows 中未见过的 0-click Preauth RCE，研究人员将其命名为 MadLicense【狂躁许可】。

这一漏洞存在于Windows远程桌面许可管理服务(RDL)中，该服务被一定程度上部署于开启Windows远程桌面(3389端口)的服务器，用于管理远程桌面连接许可。攻击者无需任何前置条件，无需用户交互(零点击)便可直接获取服务器最高权限，执行任意操作。影响所有启用 RDL 服务的 Windows Server服务器，特别是未及时更新2024年7月微软最新安全补丁的系统，已存在近30年。该漏洞可稳定利用、可远控、可勒索、可蠕虫化等，破坏力大，成功利用此漏洞可能导致易受攻击的系统完全被攻陷。

关联漏洞

1. Windows 远程桌面授权服务远程代码执行漏洞(CVE-2024-38077)

受影响版本	Windows Server 2025 Preview 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 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
影响量级	十万级
危害描述	成功利用该漏洞的攻击者可以实现远程代码执行，获取目标系统的控制权，可能导致敏感数据的泄露、以及可能的恶意软件传播。
修复措施	关闭远程桌面授权服务，该服务默认情况下并未开启，服务器对外不开放135端口。

03

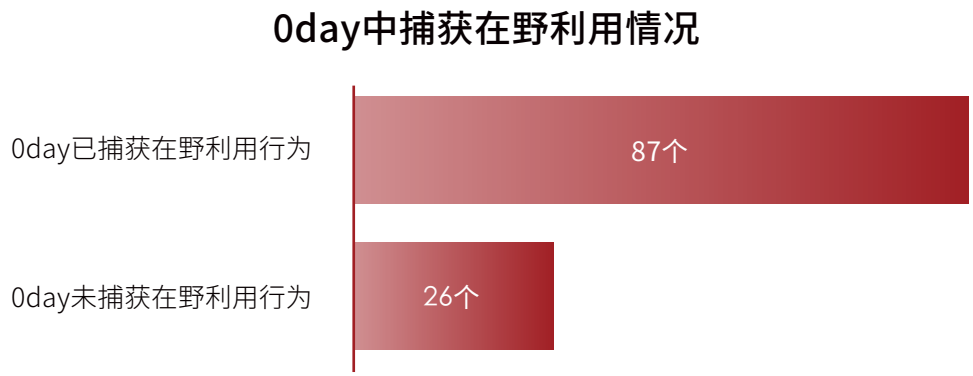
关键种类漏洞分析

第三章

一、0day漏洞

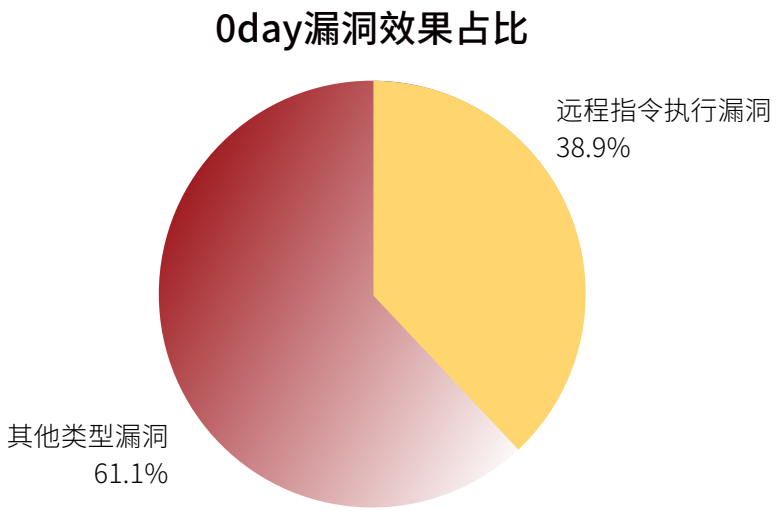
0day漏洞攻击已成为黑客常规武器，奇安信CERT在2024年新增收录 0day漏洞113个，其中被捕获到在野利用活动的占比77%，43.3%的漏洞发现公开Exploit/PoC。近1/2发现在野利用的0day漏洞没有监测到公开的利用代码，处于私有状态，仅被某些APT组织或者个人使用。但厂商对于漏洞修复的平均时长要1-2周，缩短和攻击者掌握0day漏洞的时间差迫在眉睫。

本章节回顾了2024年部分影响较大的0day漏洞，有87个0day已经捕获到在野利用行为，占比77%,如图3-1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。



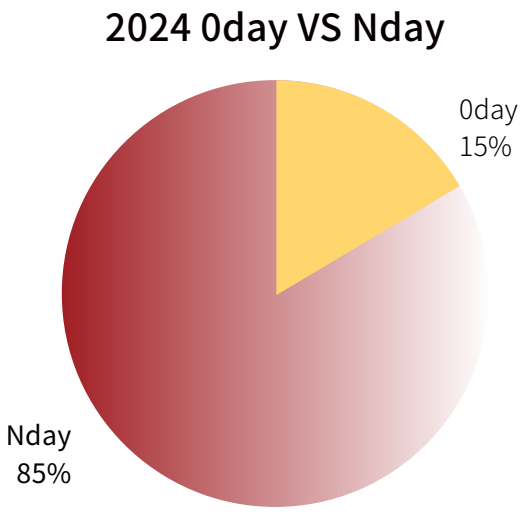
△图3-1 0day中捕获在野利用占比

在调查本年度影响重要的113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38.9%，占据近半，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3-2所示：



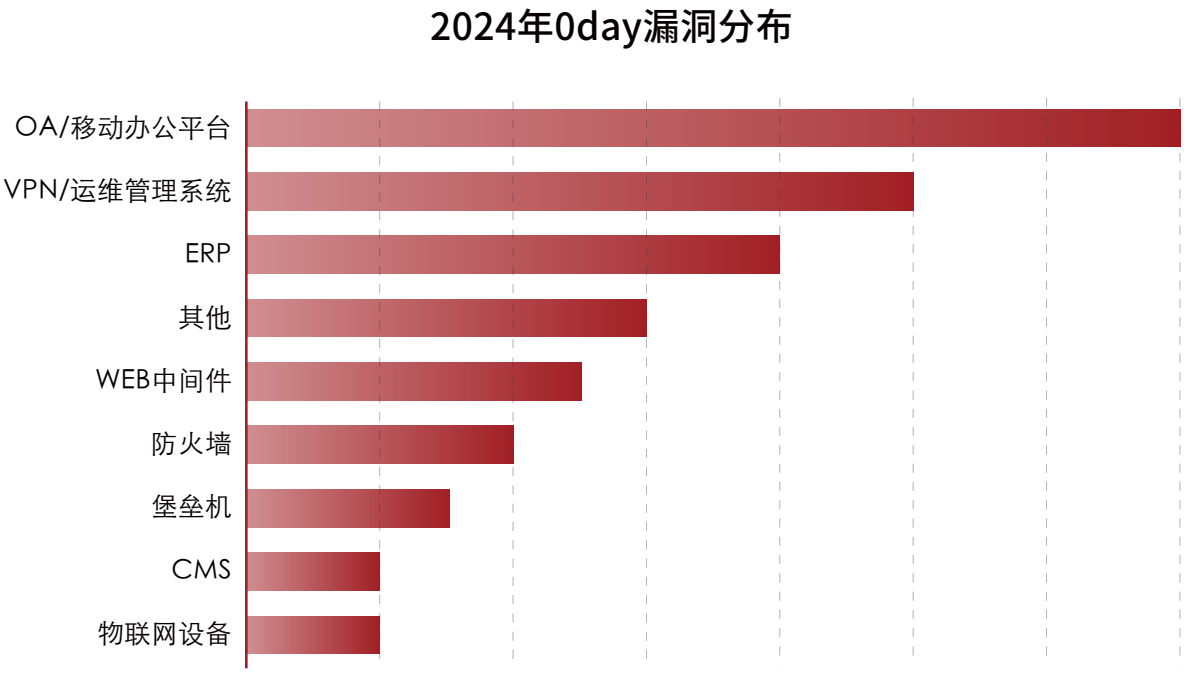
△图3-2 0day漏洞效果占比

在2023年，我们观察到 Nday 与 0day 的比例为20:80，相较2022年基本保持一致。然而在2024年，这一比例变为 15:85。鉴于零日漏洞利用率多年来稳步上升，这一变化更多源于最近对于零日漏洞使用的检测能力增强的影响，而非由于 Nday 使用率下降。对比如图3-3所示：



△图3-3 2024 0day VS Nday

在2024年攻防演练中，奇安信CERT监测到13个0day漏洞（含未公开漏洞），结合本年度已发现的0day漏洞，总结出0day漏洞分布图，如图3-4所示，其中OA漏洞占比约26%，成为攻击方最偏爱的攻击对象。



△图3-4 0day漏洞分布

1、CrushFTP 服务器端模板注入漏洞

2024年4月25日，奇安信CERT监测到CrushFTP 服务器端模板注入漏洞技术细节和POC在互联网上公开，攻击者可以通过此漏洞获得管理访问权限，泄露敏感信息或执行代码。该漏洞已被监测到在野利用事件。

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-2024-47176	十万级	代码执行	7.5	是	已公开	已公开	已发现

CrushFTP 服务器端模板注入漏洞由于CrushFTP 存在服务器端模板注入漏洞，未经身份验证的远程攻击者可以逃避虚拟文件系统(VFS)沙箱，绕过身份验证获得管理访问权限，泄露敏感信息或执行代码。

2、Nacos Derby 远程命令执行漏洞

2024年7月15日，奇安信CERT监测到Github上公开了Nacos RCE的POC工具，影响Nacos最新版本Nacos 2.3.2以及2.4.0-BETA，攻击者可通过SQL注入执行恶意代码进而获取服务器权限。7月16日，Nacos发布安全公告并建议用户开启derby运维接口鉴权机制。

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-2024-26473	万级	命令执行	9.8	是	已公开	已公开	已发现

Nacos derby远程命令执行漏洞是由于Alibaba Nacos部分版本中derby数据库默认可以未授权访问，恶意攻击者可利用此漏洞可以未授权执行SQL语句，从而远程加载恶意构造的jar包，最终导致任意代码执行从而完全控制目标系统。目前已经有利用该漏洞的在野攻击事件。
2024年7月24日，官方发布新版本并通过默认关闭derby运维接口修复该漏洞。

3、cups-browsed 远程代码执行漏洞

2024年9月24日，x用户id为evilsocket的安全研究员宣称即将在9月30日披露一个CVSS评分达到9.9的未授权远程代码执行漏洞，影响所有Linux版本。

2024年9月27日，奇安信CERT监测到cups-browsed 远程代码执行漏洞技术细节和POC在GitHub公开，影响 OpenPrinting cups-browsed 2.0.1及以下版本，攻击者可通过此漏洞在目标系统上执行任意命令进而获取服务器权限。但由于非所有Linux发行版默认安装CUPS服务以及此漏洞需要用户交互才能利用等原因，此漏洞虽然广受关注但并不能造成如预期般的危害。

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-2024-47176	十万级	代码执行	7.5	是	已公开	已公开	未发现

cups-browsed 远程代码执行漏洞是由于cups-browsed服务在处理网络打印任务时，会绑定到UDP端口631的INADDR_ANY地址，从而信任来自任何来源的数据包。这会导致未经身份验证的远程攻击者可以利用该漏洞发送特制的数据包，触发恶意请求到攻击者控制的URL，从而在目标系统上执行任意命令。
2024年10月18日，官方发布新版本2.1.0修复该漏洞。

4、Oracle WebLogic Server 远程代码执行漏洞

2024年10月15日，Oracle补丁日发布安全更新修复多个漏洞，其中Oracle WebLogic Server 远程代码执行漏洞(CVE-2024-21216)影响12.2.1.4.0和14.1.1.0.0之前版本，攻击者可利用该漏洞实现未授权远程代码执行。该漏洞于今年4月份已存在相关漏洞信息，且在7、8月份多次被安全厂商检测到在野利用。

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-2024-21216	百万级	代码执行	9.8	否	否	否	已发现

Oracle WebLogic Server 远程代码执行漏洞(CVE-2024-21216) 关键点在于利用白名单类去封装恶意类，从而二次反序列化绕过黑名单。攻击者通过T3或IIOP协议在无需用户验证的情况下远程执行代码，获取服务器权限（不需要出网），因此其危险性极高。

5、Palo Alto Networks PAN-OS 身份认证绕过漏洞 & 权限提升漏洞

2024年11月8日，Palo Alto Networks官网发布了公告(PAN-SA-2024-0015)，建议防火墙客户采取措施保护其防火墙管理接口，因为有未经证实的传言称可能存在新的漏洞。

2024年11月14日，Palo Alto Networks官网的公告更新，监测到利用未经身份验证的远程命令执行漏洞的攻击活动。
2024年11月18日，Palo Alto Networks为监测到的攻击行为已分配了CVE-2024-0012和CVE-2024-9474，攻击者可将这两个漏洞配合实现身份验证绕过并以root权限执行任意命令。

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-2024-0012	十万级	身份认证绕过	9.8	是	已公开	已公开	已发现
CVE-2024-9474		命令执行	7.2	是	已公开	已公开	已发现

Palo Alto Networks PAN-OS 身份认证绕过漏洞(CVE-2024-0012)是因为HTTP_X_PAN_AUTHCHECK参数校验不当，攻击者可通过设置off以及使用.js.map的方式来进行身份验证绕过，从而访问管理 Web 界面以及获取敏感信息。
Palo Alto Networks PAN-OS 权限提升漏洞(CVE-2024-9474)是因为将获取的$username参数直接传递给pexecute()函数拼接执行命令，具有管理员权限的攻击者可将恶意命令注入，并再次发送带有SESSION的请求以触发命令执行，从而获取防火墙root权限。

6、Windows 任务计划程序权限提升漏洞

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-2024-49039	千万级	权限提升	8.8	否	未知	未知	已发现

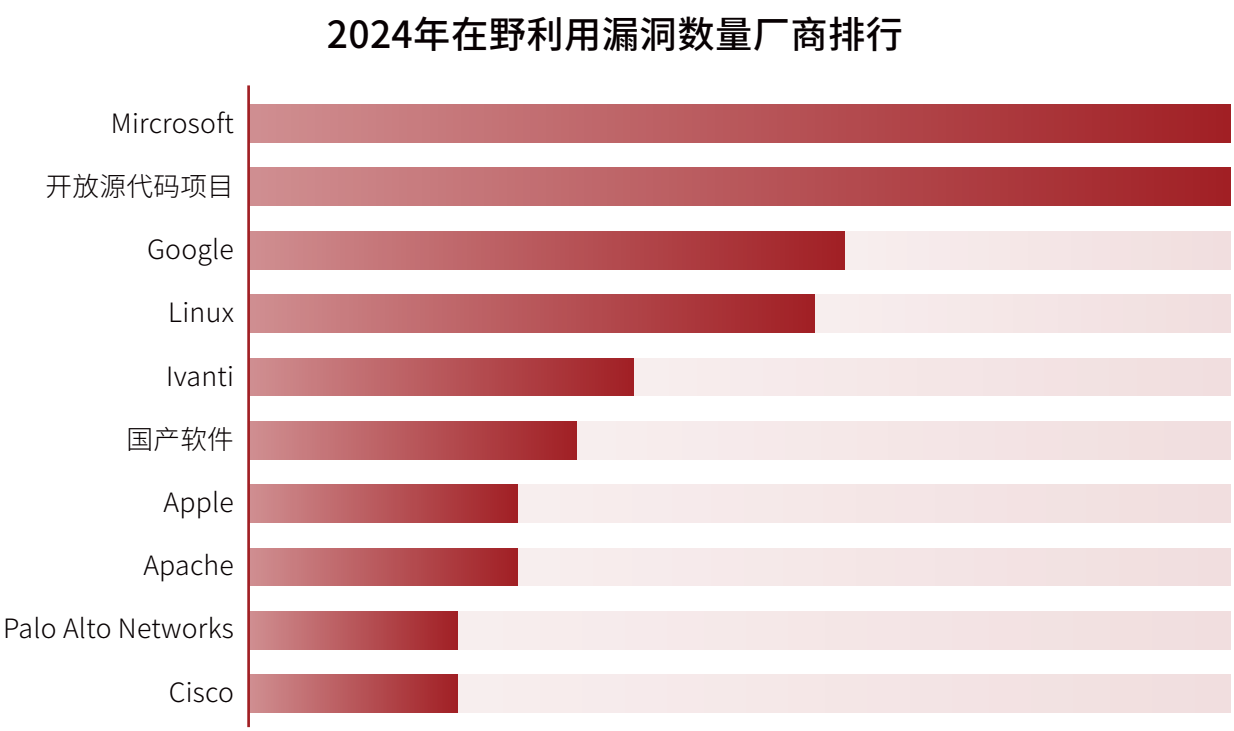
Windows Task Scheduler（任务计划程序）是Windows操作系统中的一个组件，它允许用户配置和在特定时间自动执行任务。由于 Windows 任务计划程序中的身份验证不正确，具有本地访问权限的攻击者可以通过运行特制应用程序来利用此漏洞。成功利用此漏洞将允许攻击者访问他们原本无法使用的资源并执行代码，例如远程过程调用 (RPC) 函数。此漏洞影响所有支持的 Windows 版本，并且已被检测到在野利用，威胁性较大。微软于2024年11月微软补丁日发布了该漏洞补丁。

二、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2024年，奇安信收集到以下数据：

1.监测到漏洞被实际利用（含历史真实漏洞、真实性待确认漏洞）	2.漏洞利用行为超过	3.捕获到攻击IP数量约
1200+个	30亿次	100万个

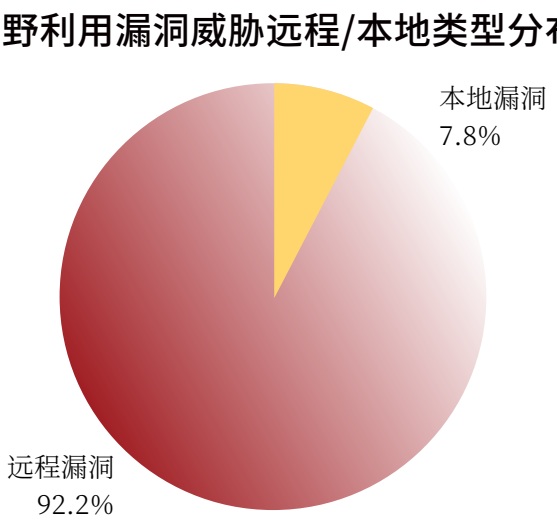
在这1200+个被实际利用的漏洞中，2024年新暴露的有343个，涉及广泛的操作系统和应用程序，排名前十位的分别是Mircrosoft、开放源代码项目、Google、Linux、Ivanti、国产软件、Apple、Apache、Palo Alto Networks、Cisco。2024年在野利用漏洞数量厂商排行如图3-5所示：



△图3-5 2024年在野利用漏洞数量厂商排行

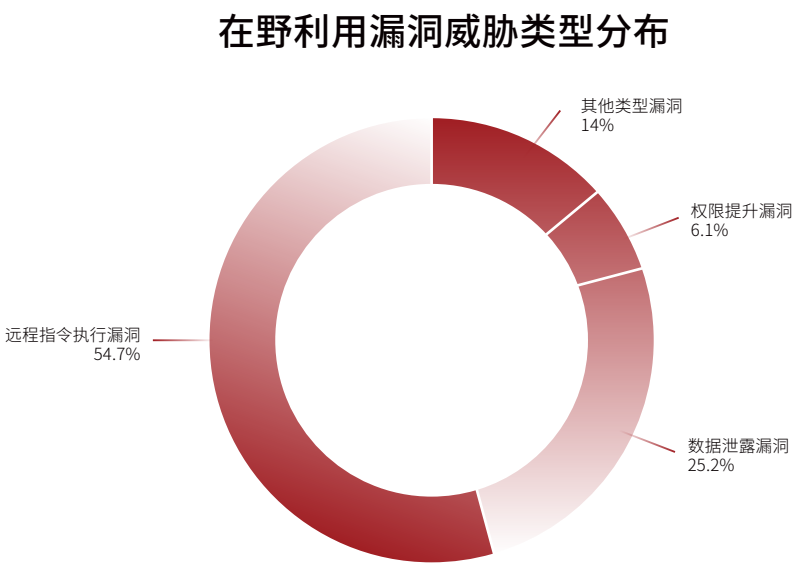
对这些现实利用的漏洞做进一步分析，得到以下结论：

远程漏洞占比92.2%，而本地漏洞仅占7.8%，在野利用漏洞威胁类型占比如图3-6所示：



△图3-6 在野利用漏洞威胁远程/本地类型分布

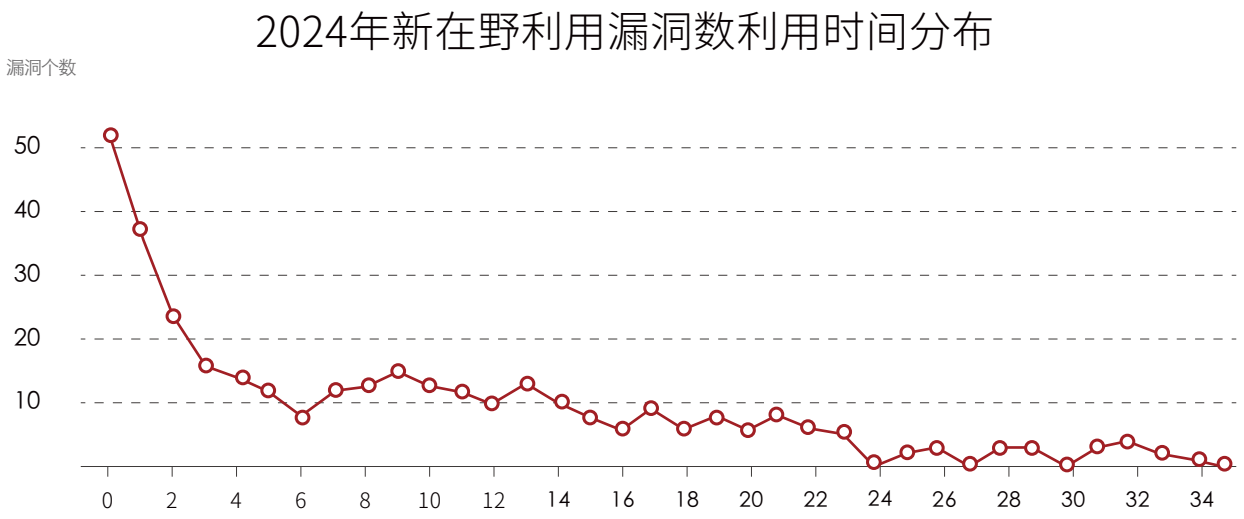
在2024年已知被利用的这些漏洞中，能够实现远程指令执行的漏洞或组合漏洞占比54.7%，比例过半，这类漏洞通常危害极高，可以被用来完全控制受影响的系统；数据泄露类型漏洞占比25.2%，这类漏洞以窃取敏感信息为主；权限提升类漏洞多为本地漏洞，占比6.1%，攻击者利用这些漏洞可以在受影响的系统中获取更高的权限。在野利用漏洞威胁类型分布如图3-7所示：



△图3-7 在野利用漏洞威胁类型分布

2024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18天，这比去年的平均时间差22天要短，有25.7%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。

68.2%的高危漏洞在发布后23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3-8所示：



△图3-8 2024年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、CrushFTP 服务器端模板注入漏洞

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-2024-21762	十万级	代码执行	9.8	是	已公开	已公开	已发现

FortiGate SSL VPN是Fortinet提供的一种远程访问解决方案，用于安全地连接远程用户和分支办公室到企业网络。SSL VPN通过加密和认证技术建立安全的远程访问连接，使用户可以安全地访问企业网络资源，如文件、应用程序和内部网站，而无需在物理上位于公司网络内部。

2024年2月8日，Fortinet 披露了FortiGate SSL VPN 代码执行漏洞(CVE-2024-21762)，这是SSL VPN中的越界写入漏洞，允许远程未经身份验证的攻击者通过特制的HTTP请求在 Fortinet SSL VPN 上执行任意代码或命令。官方称该漏洞可能正在被野外利用。

2024年 2月9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，确认已发生利用。

2、Apple iOS 与 iPadOS 多个在野高危漏洞

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-2024-23296	千万级	代码执行	7.8	否	未知	未知	已发现
CVE-2024-23225		代码执行	7.8	否	未知	未知	已发现

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。
2024年3月6日，苹果公司发布安全公告修复Apple iOS 与 iPadOS RTKit 安全特性绕过漏洞(CVE-2024-23296) 和 Apple iOS 与 iPadOS Kernel 安全特性绕过漏洞(CVE-2024-23225)，具有任意内核读写能力的攻击者可能能够绕过内核内存保护。官方称该漏洞可能已被在野利用。

3、Ivanti Cloud Service Appliance 命令注入漏洞 & 路径遍历漏洞

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-2024-8190	万级	代码执行	7.2	是	已公开	已公开	已发现
CVE-2024-8963		信息泄露	9.1	是	已公开	已公开	已发现

2024年9月10日，Ivanti官方发布公告修复了Ivanti Cloud Service Appliance 命令注入漏洞(CVE-2024-8190)。
2024年9月19日，Ivanti官方发布公告修复了Ivanti Cloud Service Appliance 路径遍历漏洞(CVE-2024-8963)。
Ivanti Cloud Service Appliance 命令注入漏洞(CVE-2024-8190)和路径遍历漏洞(CVE-2024-8963)结合使用，攻击者可以绕过管理员身份验证并在设备上执行任意命令。2024年10月11日，FortiGuard发布文章称在9月9日前已发现Ivanti CSA多个漏洞的组合在野利用。

4、Check Point Security Gateways 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-2024-24919	十万级	代码执行	7.5	是	已公开	已公开	已发现

Check Point Security Gateways 是 Check Point Software 提供的一系列网络安全解决方案。这些解决方案包括下一代防火墙（NGFW）、数据中心安全网关和 AI 驱动的量子网关，旨在为企业提供针对复杂网络威胁的先进防护。它们通过集成的威胁防护、统一的安全管理和策略控制，确保网络、云、移动和端点的安全。
2024年5月27日，Check Point官方发布了一篇博客文章，文章中声称，在发生多起涉及多家供应商的 VPN 解决方案被攻陷的攻击事件后，Check Point 一直在监控对于漏洞利用的尝试。在此监控过程中，Check Point 注意到只有“少数登录尝试”使用了启用了仅密码身份验证的本地帐户。
2024年5月28日，Check Point 官方修复了Check Point Security Gateways 任意文件读取漏洞(CVE-2024-24919)，远程攻击者可以通过构造恶意请求读取服务器上的任意文件，造成敏感信息的泄漏。

5、PHP CGI Windows平台远程代码执行漏洞

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-2024-4577	十万级	代码执行	9.8	是	已公开	已公开	已发现

PHP（Hypertext Preprocessor，超文本预处理器）是一种广泛使用的开源脚本语言，主要用于Web开发，用于生成动态网页内容。PHP的语法借鉴了C、Java、Perl等语言的特点，易于学习，并且可以快速执行。
2024年6月6日，DEVCORE发布公告披露了PHP CGI Windows平台远程代码执行漏洞(CVE-2024-4577)，未经身份认证的远程攻击者可以通过特定的字符序列绕过此前CVE-2012-1823的防护，通过参数注入攻击在远程PHP服务器上执行任意代码。2024年7月11日，FortiGuard发布文章称在漏洞披露后的24小时内就出现了该漏洞的在野利用尝试，此后又多次发现黑客组织利用此漏洞进行攻击。

6、Rejetto HTTP File Server 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-2024-23692	十万级	代码执行	7.2	是	已公开	已公开	已发现

HFS（HTTP File Server）是一个简单易用的文件服务器软件，用户可以通过直观的 web 界面来管理文件和目录的共享。

HFS（HTTP File Server）存在模板注入漏洞，未经身份验证的攻击者通过发送特制的 HTTP 请求在受影响的系统上执行任意命令。2024年6月6日，Rejetto HTTP File Server 模板注入漏洞(CVE-2024-23692)被一位安全研究员在博客文章中披露，此时该漏洞EXP已经被广泛传播。

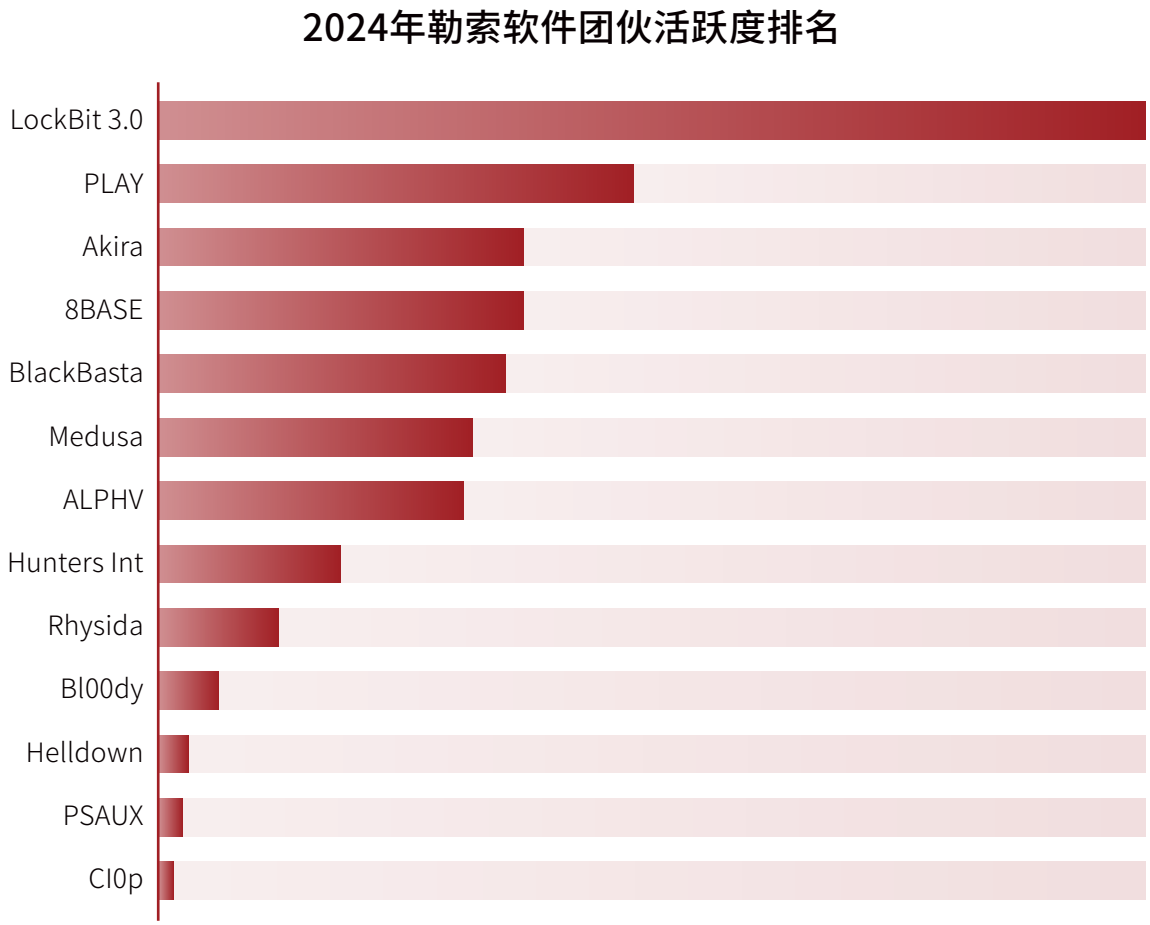
三、勒索软件相关漏洞

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，2024年多个漏洞在公开后立即遭到勒索软件攻击者滥用。

Black Basta和Bl00dy勒索软件团伙被披露利用远程桌面管理软件ScreenConnect存在的漏洞CVE-2024-1708和CVE-2024-1709发起攻击。Black Basta勒索团伙利用漏洞后部署了Cobalt Strike木马，而Bl00dy勒索团伙在攻击活动中使用了此前Conti和LockBit Black（即LockBit 3.0）泄露的构建器。

了解勒索软件攻击中利用的主要漏洞对企业安全防护能力建设至关重要。通过优先考虑漏洞缓解、及时应用补丁并遵循网络安全准则，可以降低成为勒索软件攻击受害者的风险。

勒索软件团伙活跃度排名如图3-9所示。



△图3-9 2024年勒索软件团伙活跃度排名

2024年流行勒索软件关联漏洞如下所示。本节全面总结2024年勒索软件攻击中利用的关键漏洞，强调主动预防风险和有效事件响应的必要性。

1.Black Basta 和 Bl00dy利用ScreenConnect漏洞

2024年2月19日，ConnectWise公司公布了其ScreenConnect软件存在的两个重大安全漏洞，分别是CVE-2024-1708和CVE-2024-1709，这两个漏洞影响的版本包括23.9.7及之前的版本。这些安全漏洞可能允许黑客在未经授权的情况下获得系统的访问和控制权限。

2024年2月21日，美国网络安全和基础设施安全局将该漏洞添加到其已知被利用漏洞目录中。在此期间研究人员多次追踪到涉及CVE-2024-1708和CVE-2024-1709漏洞的勒索软件攻击，其中主要包括Black Basta 和 Bl00dy 勒索软件集团。

关联漏洞

ConnectWise ScreenConnect 路径遍历漏洞(CVE-2024-1708)
Connectwise Screenconnect 身份认证绕过漏洞(CVE-2024-1709)

受影响版本	23.9.7 及更早版本（低权限用户可以执行任意代码）
影响量级	万级
危害描述	允许攻击者执行远程代码或直接影响机密数据或关键系统的能力。
修复措施	受影响用户升级至最新版本：ConnectWise ScreenConnect >= 23.9.8

2.多个组织积极利用JetBrains TeamCity漏洞发起供应链攻击

2024 年 3 月 4 日，JetBrains发布了一篇博客文章，发布了针对两个身份验证绕过漏洞（CVE-2024-27198和CVE-2024-27199）的安全补丁。不久，Rapid7 团队发布了影响 TeamCity JetBrains 的漏洞的初步利用代码。

由于之前曾有俄罗斯外情局(SVR)等在内的国家级攻击者利用JetBrains的漏洞实施供应链攻击，此次漏洞被积极利用的情报尤显重要。该公司还观察到黑市上犯罪分子利用这些漏洞进行初始访问的销售。

关联漏洞

JetBrains TeamCity 身份验证绕过漏洞(CVE-2024-27198)
JetBrains TeamCity 路径遍历漏洞(CVE-2024-27199)

受影响版本	JetBrains TeamCity < 2023.11.4
影响量级	十万级
危害描述	未经身份验证的远程攻击者利用漏洞CVE-2024-27198可以绕过系统身份验证，完全控制所有TeamCity项目、构建、代理和构件，为攻击者执行供应链攻击提供便利；利用漏洞CVE-2024-27199则可以进一步对系统的敏感数据进行非法访问。
修复措施	受影响用户升级至最新版本：ConnectWise ScreenConnect >= 23.9.8

3.Akira和Fog勒索软件利用Veeam RCE漏洞

2024年9月4日，备份和恢复软件提供商Veeam发布了安全公告披露了一个严重的未经身份验证的远程代码执漏洞CVE-2024-40711，之前影响该软件的几个高危漏洞均被广泛利用。

2024年10月17日，美国网络安全和基础设施安全局将该漏洞添加到其已知被利用漏洞目录中。在此期间研究人员多次追踪到涉及CVE-2024-40711漏洞的勒索软件攻击，其中包括Akira和Fog等勒索软件。

关联漏洞

Veeam Backup & Replication 反序列化漏洞(CVE-2024-40711)

受影响版本	12.1.2.172 及更早版本（低权限用户可以执行任意代码） 12.1.1.56 及更早版本（未经身份验证的 RCE 攻击）
影响量级	十万级
危害描述	未经身份验证的攻击者可远程代码执行获取服务器权限。
修复措施	升级Veeam Backup & Replication到安全版本

4.VMware ESXi成为多个勒索软件攻击目标

2024年7月29日，微软发布了一篇威胁情报博客，介绍了观察到VMware ESXi身份认证绕过漏洞(CVE-2024-37085)的利用情况，微软确定了三种利用该漏洞的方法：将ESX 管理员组添加到域并向其中添加用户、将域中的任何组重命名为ESX 管理员，并将用户添加到该组或使用现有组成员、ESXi 虚拟机管理程序权限刷新。

VMware ESXi在Hunter测绘中有接近100万资产，此漏洞被许多勒索软件组织用作入侵后攻击技术，包括BlackByte、Storm-0506、Storm-1175、Octo Tempest 和 Manatee Tempest。

关联漏洞

VMware ESXi 身份认证绕过漏洞(CVE-2024-37085)

受影响版本	8.x<=VMware ESXi<ESXi80U3-24022510 VMware ESXi==7.x VMware Cloud Foundation==4.x 5.x<=VMware Cloud Foundation<=5.2
影响量级	百万级
危害描述	该漏洞影响VMware ESXi虚拟机管理程序的Active Directory集成身份验证，攻击者可获取对域加入的ESXi虚拟机管理程序的完全管理权限。
修复措施	1.验证组ESX Admins是否存在于域中并且已得到强化。 2.通过更改 ESXi 虚拟机管理程序本身的设置来手动拒绝此组的访问。如果不需要 Active Directory ESX 管理员组的完全管理员访问权限，则可以使用高级主机设置“Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd”禁用此行为。 3.将管理组更改为 ESXi 虚拟机管理程序中的其他组。

5.Zyxel 防火墙的第二个漏洞在 Helldown 勒索软件攻击中被利用

新出现的Helldown勒索软件操作利用Zyxel防火墙中的漏洞，成功入侵企业网络，窃取数据并加密设备。尽管不是勒索软件领域的主要参与者，但 Helldown 自夏季推出以来迅速发展，在其数据勒索门户网站上有众多受害者。

Helldown勒索软件首次被Cyfirma于2024年8月9日记录，随后Cyberint于10月13日再次提及。该勒索软件的Linux变种专门针对VMware文件，显示出其加密功能尚未完全开发。

列出的受害者之一是网络和网络安全解决方案提供商 Zyxel Europe。该组织的加密器看起来并不是非常先进，威胁者利用批处理文件来结束任务，而不是直接将此功能合并到恶意软件中。

关联漏洞

Zyxel ZLD 防火墙目录遍历漏洞(CVE-2024-11667)

受影响版本	5.00 <= Zyxel ZLD 防火墙固件版本 <= 5.38
影响量级	十万级
危害描述	攻击者可以通过精心设计的 URL 下载或上传文件。 zyxel-security-advisory-protecting-against-recent-firewall-threats-11-27-2024
修复措施	建议用户尽快升级至安全版本。

6.大规模 PSAUX 勒索软件攻击CyberPanel 实例漏洞

超过 22,000 个 CyberPanel 实例在线暴露于严重的远程代码执行 (RCE) 漏洞，在一次 PSAUX 勒索软件攻击中，几乎所有实例都遭到离线攻击。

安全研究员 DreyAnd 透露，CyberPanel 2.3.6（可能还有 2.3.7）存在两个不同的安全问题，可能导致未经身份验证的远程根访问被利用。

PSAUX 勒索软件自 2024 年 6 月以来一直存在，通过漏洞和错误配置来攻击暴露的 Web 服务器。由于 PSAUX 勒索软件加密文件的方式存在缺陷，因此可以使用LeakIX创建的解密器免费解密文件。LeakIX现已告诉 BleepingComputer，威胁行为体大规模利用暴露的 CyberPanel 服务器来安装PSAUX 勒索软件。安全专家推测，攻击者可能利用了未及时修补的两个漏洞。

关联漏洞

CyberPanel upgrademysqlstatus 远程命令执行漏洞(CVE-2024-51567)

受影响版本	CyberPanel v2.3.5 CyberPanel v2.3.6
影响量级	万级
危害描述	该漏洞源于upgrademysqlstatus接口未做身份验证和参数过滤，未授权攻击者可执行任意命令获取服务器权限。
修复措施	建议用户尽快升级至安全版本。

关联漏洞

CyberPanel 权限提升漏洞(CVE-2024-51378)

受影响版本	CyberPanel = v2.3.5 CyberPanel < v2.3.6
影响量级	十万级
危害描述	该漏洞允许远程攻击者绕过身份验证并执行任意命令。攻击者可以通过/dns/getresetstatus或/ftp/getresetstatus绕过仅适用于POST请求的 secMiddleware，并在statusfile属性中使用shell元字符。
修复措施	建议用户尽快升级至安全版本。

四、APT活动相关漏洞

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。本节回顾了2024年部分影响较大的APT事件相关漏洞。

1、Jenkins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-2024-23897	十万级	**信息泄露 代码执行**	9.8	是	已公开	已公开	未发现

2024年1月24日，Jenkins官方发布了安全公告，确认修复了任意文件读取导致的任意代码执行漏洞。Jenkins用于处理CLI命令的命令解析器中的expandAtFile功能存在任意文件读取漏洞，未经身份认证的远程攻击者利用该漏洞可以读取部分文件的有限行内容，远程攻击者经过身份验证或目标Jenkins更改了默认”Security”配置可以通过该漏洞读取任意文件，进一步利用该漏洞并结合其他功能可能导致任意代码执行。APT组织RansomEXX曾利用此漏洞对印度银行业发起过大规模的勒索软件攻击并窃取了大量的用户数据。

2、Internet快捷方式文件安全特性绕过漏洞

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-2024-21412	千万级	**安全特性绕过代码执行**	8.1	是	已公开	已公开	已发现

2024年2月14日，奇安信CERT监测到微软二月补丁日修复多个漏洞，其中包括Internet快捷方式文件安全特性绕过漏洞(CVE-2024-21412)。未经身份认证的远程攻击者通过该漏洞制作恶意文件并发送给受害者，诱导受害者打开后将触发该漏洞，绕过安全检查并执行恶意代码。

该漏洞于2023年12月下旬被攻击团伙Water Hydra作为0day进行在野攻击活动，此团伙主要针对全球银行、加密货币平台、外汇和股票交易平台、赌博网站和赌场等目标进行攻击。在此攻击链中，威胁行为体利用CVE-2024-21412 绕过 Microsoft Defender SmartScreen 并使用 DarkMe 恶意软件感染受害者。

3、WPS Office 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-2024-7262	千万级	代码执行	7.8	是	已公开	已公开	已发现

2024年2月29日，CVE-2024-7262漏洞利用文档已上传至 VirusTotal，后续官方发布静默补丁解决了部分错误代码，但其余有缺陷的代码仍然可被利用。5月底 ESET研究人员报告相关信息，官方确认修复该漏洞。

该漏洞允许攻击者通过操纵 WPS Office 插件promecefpluginhost.exe中的文件路径上传恶意 DLL，从而实现远程代码执行。韩国网络间谍组织APT-C-60利用该漏洞在东亚地区部署了SpyGlace 后门。

4、Windows DWM 核心库权限提升漏洞

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-2024-30051	千万级	代码执行	7.8	是	已公开	已公开	已发现

2024年4月1日，该漏洞被发现在一份上传到VirusTotal上的漏洞简单分析报告。相关报告中的漏洞特征和实际样本指向了QakBot。QakBot又称为QBot、QuackBot、Pinkslipbot，是一款已经存在十余年的银行木马，于2007年在野外被发现，此后一直在持续维护和发展。近十年来，没有发现过QakBot相关攻击中使用0day的案例，直到出现该漏洞。

该漏洞是由于主 Windows DWM 库dwmcore.dll中的整数除法中存在大小计算错误而导致。本地用户可以在dwmcore.dll中的CCommandBuffer::Initialize方法中导致堆上的缓冲区溢出，并可以使用具有 Integrity 系统权限的DWM用户执行任意代码。

5、Magento Open Source XML外部实体注入漏洞

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-2024-34102	十万级	代码执行	9.8	是	已公开	已公开	未发现

自 6 月份披露该漏洞以来，许多企业并未理会对其严重性的警告。尽管 Adobe 于 7 月 8 日将该漏洞定性为严重漏洞，并发布了手动删除过期密钥的指南，但数千家商店仍然暴露在漏洞之下。在今年夏天，七家黑客组织利用此漏洞入侵了大约 5% 的 Adobe Commerce 和 Magento 商店，影响了超过 4,275 家在线零售商，其中包括 Ray-Ban、国家地理、思科、惠而浦和 Segway 等知名品牌。

Adobe Commerce和Magento Open Source的受影响版本存在XML外部实体引用（XXE）的不当限制漏洞，这可能导致任意代码执行。攻击者可以通过发送一个引用外部实体的精心构造的XML文档来利用这个漏洞，造成敏感信息泄露或远程代码执行。

五、其它类别关键漏洞

1、GitLab 密码重置漏洞

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-2023-7028	十万级	身份认证绕过	10.0	是	已公开	已公开	未知

GitLab 是一个基于Web的开源代码托管平台，提供了代码仓库管理、问题跟踪、持续集成和部署等功能。2024年1月11日，GitLab官方发布安全公告，修复了一个无需用户交互即可通过密码重置接管帐户的漏洞，用户帐户密码重置电子邮件可能会发送到未经验证的电子邮件地址。

2024年1月13日，Github上公开了GitLab密码重置漏洞POC，未经身份验证的远程攻击者可以利用该漏洞将用户帐户密码重置电子邮件发送至任意目标电子邮箱。LDAP 用户不会受到影响，因为他们没有忘记/重置密码选项。此外，启用了双因素身份验证的用户很容易受到密码重置的影响，但帐户不会被接管，因为他们需要第二个身份验证因素才能登录。

2、Atlassian Confluence 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-2023-22527	十万级	代码执行	10.0	是	已公开	已公开	已发现

Atlassian Confluence 是一款企业知识管理和协作工具，旨在帮助团队共享知识、协作和合作。Confluence提供了一个集中式的平台，使团队成员可以创建、共享和协作文档、项目计划、会议记录等内容。2024年1月16日，Atlassian官方发布漏洞公告：Confluence Data Center 和 Server 的旧版本中存在模板注入漏洞，未经身份验证的攻击者可利用该漏洞在受影响的版本上实现 RCE。

2024年1月22日，该漏洞细节和POC公开，立即被进行大规模扫描和尝试利用，并在随后几个月持续被勒索软件以及加密货币挖矿活动等利用。

3、SolarWinds Serv-U 目录遍历漏洞

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-2024-28995	十万级	信息泄露	7.5	是	已公开	已公开	已发现

SolarWinds Serv-U 是一款用于文件传输和安全文件共享的软件解决方案。Serv-U提供了可靠的文件传输服务，支持FTP、SFTP、FTPS和HTTP/S协议，旨在帮助组织安全地共享文件并满足合规性要求。2024年6月5日，SolarWinds披露了CVE-2024-28995，这是一个高严重性目录遍历漏洞，成功利用此漏洞可让未经身份验证的攻击者读取目标服务器上的敏感文件。

该漏洞很容易被利用，并且允许外部未经身份验证的攻击者读取磁盘上的任何文件，包括二进制文件等，只要他们知道路径并且文件未被锁定。6月13日，该漏洞细节和POC已公开。7月17日被添加到美国网络安全和基础设施安全局的已知被利用漏洞 (KEV) 列表中。

4、Microsoft Outlook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-2024-21413	千万级	信息泄露代码执行	9.8	是	已公开	已公开	未发现

Microsoft Office Outlook是微软办公软件套装的组件之一，它对Windows自带的Outlook express的功能进行了扩充。Outlook的功能很多，可以用它来收发电子邮件、管理联系人信息、记日记、安排日程、分配任务。微软二月补丁日中发布了Microsoft Outlook远程代码执行漏洞(CVE-2024-21413)的补丁，成功利用此漏洞将允许攻击者绕过Office受保护视图，并在编辑模式下打开文件，而不是在保护模式下，预览窗格也可触发此漏洞。

2024年2月23日，该漏洞技术细节与PoC在互联网上公开，未经身份验证的远程攻击者可以诱骗受害者打开特制文件利用此漏洞在目标系统上执行任意代码。

5、JetBrains TeamCity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-2024-27198	十万级	身份验证绕过	9.8	是	已公开	已公开	未发现

JetBrains TeamCity是一款由JetBrains开发的持续集成和持续交付（CI/CD）服务器。它提供了一个功能强大的平台，用于自动化构建、测试和部署软件项目。TeamCity旨在简化团队协作和软件交付流程，提高开发团队的效率和产品质量。

2024年3月4日，JetBrains TeamCity发布新版本修复了两个高危漏洞JetBrains TeamCity 身份验证绕过漏洞(CVE-2024-27198)与JetBrains TeamCity 路径遍历漏洞(CVE-2024-27199)。未经身份验证的远程攻击者利用CVE-2024-27198可以绕过系统身份验证，完全控制所有TeamCity项目、构建、代理和构件，为攻击者执行供应链攻击。

2023年9月，APT29曾利用一个类似的漏洞CVE-2023-42793进行过在野攻击。2024年3月6日，该漏洞细节和POC公开。

6、Adobe ColdFusion 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-2024-20767	十万级	信息泄露	8.2	是	已公开	已公开	未发现

Adobe ColdFusion是美国Adobe公司的一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言，将可扩展、改变游戏规则且可靠的产品的愿景变为现实。2024年3月12日，Adobe ColdFusion发布新版本修复了Adobe ColdFusion 任意文件读取漏洞(CVE-2024-20767)，未经身份认证的远程攻击者可以构造恶意请求读取目标服务器上的任意文件，从而泄露敏感信息。3月26日，该漏洞细节和POC在GitHub公开。

04

2025年漏洞新兴技术发展趋势展望

第四章

一、人工智能（AI）与自动化漏洞挖掘技术

2025年，人工智能在漏洞挖掘和利用中的应用将进一步扩大，既为网络攻防带来便利，也产生了新的安全风险：

1.AI驱动的自动化漏洞挖掘

攻击者使用AI生成的工具大规模扫描和分析目标系统代码，自动发现复杂漏洞。

AI生成的代码审计工具可以通过语义分析发现逻辑缺陷，如路径遍历、数据注入等漏洞。

预计2025年，AI驱动的漏洞挖掘将使高风险漏洞的发现时间缩短30%-40%。

2.AI定向利用漏洞

攻击者利用AI训练模型生成最优攻击链，针对目标构建量身定制的攻击手段。

举例：AI可根据目标防御配置动态选择攻击路径，避免触发防御机制。

3.AI生成代码的漏洞隐患

随着AI生成工具（如ChatGPT Code Interpreter）在开发领域的应用，自动生成的代码可能包含潜在漏洞，攻击者可以通过诱导AI生成具有安全缺陷的代码插入关键系统。

应对措施：企业需部署AI辅助的漏洞检测工具，并加强对AI生成代码的安全审计。

二、量子计算影响下的密码学漏洞

量子计算能力的逐步突破可能对传统密码学算法形成颠覆性威胁，并引发以下漏洞风险：

1.传统加密算法的失效

量子计算可以通过Shor算法快速破解传统公钥密码（如RSA、ECC），导致加密通信漏洞。

攻击者可通过量子计算能力窃取加密通信内容并解密敏感数据。

2.量子安全协议中的漏洞

在现有量子通信协议中，量子密钥分发（QKD）协议的实现可能存在物理漏洞，攻击者可通过侧信道攻击窃取密钥。

3.新型量子算法中的安全问题

量子计算技术的发展也可能催生新的算法漏洞，特别是早期的量子密码算法实现中容易出现逻辑缺陷。

应对措施：推动量子抗性算法（PQC）的标准化，同时加强对量子通信协议的安全审查。

三、云原生架构与虚拟化漏洞趋势

随着云原生架构的普及以及虚拟化技术的深入应用，2025年的云计算环境将面临更多的漏洞威胁：

1.容器与Kubernetes漏洞

容器逃逸漏洞仍是攻击云原生环境的主要手段，攻击者利用容器与主机之间的隔离不足，获取底层权限。Kubernetes集群的配置错误或认证机制漏洞将被广泛利用，导致攻击者接管整个集群。

2.无服务器计算（Serverless）漏洞

无服务器架构中，由于函数隔离不足，攻击者可以通过利用共享资源（如CPU或内存）进行横向扩展。

3.虚拟化漏洞

虚拟机管理程序（Hypervisor）和虚拟化环境的漏洞利用会显著增加，特别是AMD SEV和Intel SGX等硬件隔离技术的实现漏洞，将成为攻击突破点。

应对措施：加强对云原生组件的安全配置和漏洞扫描，推行零信任架构（Zero Trust）。

四、物联网设备漏洞与攻击面扩展

2025年，物联网设备漏洞暴露的趋势将愈加严峻，主要表现在：

1.物联网设备固件漏洞

物联网设备固件中因代码质量不高，漏洞数量剧增，攻击者可通过反编译固件获取敏感信息或注入恶意代码。

2.物联网协议漏洞

物联网通信协议（如MQTT、CoAP）中缺乏强认证和加密，可能导致攻击者拦截通信或伪装为合法设备。

3.跨领域传播的攻击链

攻击者通过智能家居、工业控制设备的漏洞切入企业网络，形成物联网到IT基础设施的攻击链，进一步扩大攻击范围。

应对措施：加强物联网设备的固件安全升级机制，推动物联网安全标准化。

五、自动化漏洞利用与攻击工具的进化

2025年，漏洞利用工具的自动化、模块化水平将进一步提高：

1.漏洞利用工具自动化

开源漏洞利用框架（如Metasploit）将集成更多AI算法，使得漏洞利用门槛进一步降低。

自动化工具可快速生成多种利用方式，并动态调整Payload以适应不同目标。

2.漏洞市场的产业化

攻击者在暗网中交易自动化利用工具和漏洞利用即服务（Exploitation-as-a-Service），导致漏洞威胁规模化发展。

应对措施：安全团队需持续追踪漏洞利用工具的发展动向，并通过威胁情报获取相关工具的特征信息，提前部署防御策略。

05

漏洞处置建议

第五章

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

总结

第六章

2024年漏洞态势表明，漏洞数量持续增长，威胁全面升级，重点领域漏洞爆发，行业威胁显著，漏洞利用手段趋于复杂化和隐蔽化，漏洞利用已成为攻击者实现目标的核心手段。展望2025年，AI、量子计算、云原生技术和物联网的快速发展将进一步扩展漏洞威胁面，同时也对网络防御提出更高要求。企业需及时调整安全策略，通过技术升级、自动化管理和威胁情报支持构建主动防御体系，以应对日益复杂的漏洞威胁环境。

07

奇安信漏洞情报服务订阅

第七章

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33万余条漏洞信息，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）

附录1：2024年0DAY漏洞列表

更新日期	公开日期	漏洞名称	危险等级	威胁类型	编号
2024/12/26	2024/11/20	Apple 多款产品输入验证错误漏洞 (CVE-2024-44308)	高危	代码执行 安全特性绕过	CVE-2024-44308
2024/12/26	2024/11/20	Apple 多款产品跨站脚本漏洞(CVE-2024-44309)	中危	代码执行	CVE-2024-44309
2024/12/21	2024/11/18	Palo Alto Networks PAN-OS 身份认证绕过漏洞(CVE-2024-0012)	极危	身份认证绕过	CVE-2024-0012
2024/12/3	2024/11/18	Oracle Agile PLM Framework 授权不当漏洞 (CVE-2024-21287)	高危	信息泄露	CVE-2024-21287
2024/12/21	2024/11/18	Palo Alto Networks PAN-OS 权限提升漏洞 (CVE-2024-9474)	高危	命令执行	CVE-2024-9474
2024/12/6	2024/11/15	GeoVision 多款产品命令执行漏洞 (CVE-2024-11120)	极危	命令执行	CVE-2024-11120
2024/12/21	2024/11/12	Windows NTLM 哈希泄露欺骗漏洞 (CVE-2024-43451)	中危	安全特性绕过	CVE-2024-43451
2024/12/21	2024/11/12	Windows 任务计划程序权限提升漏洞 (CVE-2024-49039)	高危	权限提升	CVE-2024-49039
2024/12/9	2024/10/29	CyberPanel 权限提升漏洞 (CVE-2024-51378)	极危	命令执行	CVE-2024-51378
2024/12/26	2024/10/27	CyberPanel upgrademy-sqlstatus 远程命令执行漏洞(CVE-2024-51567)	极危	命令执行	CVE-2024-51567
2024/11/29	2024/10/23	Cisco ASA 和 FTD 拒绝服务漏洞(CVE-2024-20481)	中危	代码执行 拒绝服务 信息泄漏	CVE-2024-20481
2024/12/5	2024/10/23	Fortinet FortiManager 身份认证绕过漏洞 (CVE-2024-47575)	极危	身份认证绕过	CVE-2024-47575

更新日期	公开日期	漏洞名称	危险等级	威胁类型	编号
2024/11/29	2024/10/21	ScienceLogic SL1 远程代码执行漏洞 (CVE-2024-9537)	极危	代码执行	CVE-2024-9537
2024/12/30	2024/10/9	Mozilla Firefox Animation timelines 释放后重用漏洞 (CVE-2024-9680)	高危	代码执行	CVE-2024-9680
2024/11/29	2024/10/8	Ivanti CSA信息泄露漏洞 (CVE-2024-9381)	高危	拒绝服务 代码执行 信息泄露	CVE-2024-9381
2024/11/29	2024/10/8	Ivanti CSA SQL注入漏洞 (CVE-2024-9379)	中危	代码执行 信息泄露	CVE-2024-9379
2024/11/29	2024/10/8	Ivanti CSA 操作系统命令注入漏洞(CVE-2024-9380)	高危	命令执行	CVE-2024-9380
2024/12/28	2024/10/8	Windows MSHTML 平台欺骗漏洞 (CVE-2024-43573)	中危	代码执行	CVE-2024-43573
2024/12/28	2024/10/8	Microsoft Management Console 远程代码执行漏洞(CVE-2024-43572)	高危	权限提升 拒绝服务 信息泄露 代码执行	CVE-2024-43572
2024/11/29	2024/10/7	Samsung Exynos安全漏洞(CVE-2024-44068)	高危	拒绝服务 代码执行	CVE-2024-44068
2024/11/29	2024/10/7	高通芯片DSP服务 释放后重用漏洞 (CVE-2024-43047)	高危	拒绝服务 代码执行	CVE-2024-43047
2024/11/29	2024/9/19	Ivanti Cloud Service Appliance 路径遍历漏洞 (CVE-2024-8963)	极危	信息泄露 代码执行 拒绝服务	CVE-2024-8963
2024/11/29	2024/9/11	Windows MSHTML 平台欺骗漏洞 (CVE-2024-43461)	高危	信息泄露	CVE-2024-43461
2024/11/29	2024/9/11	Windows Installer 权限提升漏洞(CVE-2024-38014)	高危	权限提升	CVE-2024-38014
2024/11/29	2024/9/11	Microsoft Windows 更新远程代码执行漏洞 (CVE-2024-43491)	极危	拒绝服务 代码执行	CVE-2024-43491
2024/11/29	2024/9/11	Microsoft Publisher 安全特性绕过漏洞 (CVE-2024-38226)	高危	安全特性绕过	CVE-2024-38226

更新日期	公开日期	漏洞名称	危险等级	威胁类型	编号
2024/12/1	2024/9/11	Windows Mark of the Web 安全特性绕过漏洞 (CVE-2024-38217)	中危	安全特性绕过	CVE-2024-38217
2024/11/29	2024/9/10	Adobe Acrobat & Reader 释放后重用漏洞 (CVE-2024-41869)	高危	代码执行 拒绝服务	CVE-2024-41869
2024/11/29	2024/8/22	Versa Director 危险文件类型上传漏洞 (CVE-2024-39717)	中危	代码执行	CVE-2024-39717
2024/11/29	2024/8/21	Google Chrome 缓冲区溢出漏洞(CVE-2024-7965)	高危	身份认证绕过	CVE-2024-7965

注：以上仅展示部分漏洞，点击下载完整列表：

2024年0DAY漏洞列表.csv

（超链接：https://ti.qianxin.com/api/d/c6MRFk）

附录2：2024年在野利用漏洞列表

公开日期	发现在野利用日期	漏洞名称	危险等级	威胁类型	编号
2024/12/27	2024/12/30	Palo Alto Networks PAN-OS 拒绝服务漏洞 (CVE-2024-3393)	高危	拒绝服务	CVE-2024-3393
2024/12/18	2024/12/20	Linux Kernel 越界访问漏洞(CVE-2024-46859)	高危	代码执行 信息泄露	CVE-2024-46859
2024/12/17	2024/12/18	Docker CE AuthZ 权限提升漏洞(CVE-2024-41110)	高危	权限提升 身份认证绕过	CVE-2024-41110
2024/12/17	2024/12/24	BeyondTrust 命令注入漏洞(CVE-2024-12356)	极危	命令执行	CVE-2024-12356
2024/12/13	2024/12/17	GStreamer 越界写入漏洞 (CVE-2024-47541)	中危	拒绝服务 信息泄露	CVE-2024-47541
2024/12/13	2024/12/26	Cleo 多款产品任意文件上传漏洞(CVE-2024-55956)	极危	代码执行	CVE-2024-55956
2024/12/12	2024/12/14	Oracle Java SE 可访问数据未授权访问漏洞 (CVE-2024-21235)	中危	信息泄露	CVE-2024-21235
2024/12/12	2024/12/25	GStreamer 越界写入漏洞 (CVE-2024-47615)	高危	拒绝服务 信息泄露	CVE-2024-47615
2024/12/11	2024/12/26	Apache Struts 文件上传漏洞(CVE-2024-53677)	高危	代码执行	CVE-2024-53677
2024/12/10	2024/12/31	Linux Kernel 信息泄露漏洞(CVE-2024-47685)	极危	拒绝服务 信息泄露	CVE-2024-47685
2024/12/10	2024/12/31	Linux Kernel 拒绝服务漏洞(CVE-2024-47674)	中危	拒绝服务 信息泄露	CVE-2024-47674
2024/12/10	2024/12/11	Windows 通用日志文件系统驱动程序权限提升漏洞 (CVE-2024-49138)	极危	命令执行	CVE-2024-53899
2024/12/10	2024/12/31	Virtualenv 命令注入漏洞 (CVE-2024-53899)	高危	权限提升	CVE-2024-53899

公开日期	发现在野利用日期	漏洞名称	危险等级	威胁类型	编号
2024/12/5	2024/12/31	PHP 整数溢出漏洞 (CVE-2024-11236)	极危	拒绝服务 信息泄露 代码执行	CVE-2024-11236
2024/12/2	2024/12/31	HTTP/2 拒绝服务漏洞 (CVE-2023-45288)	高危	拒绝服务	CVE-2023-45288
2024/12/2	2024/12/31	HashiCorp go-retryable-http 信息泄露漏洞 (CVE-2024-6104)	中危	信息泄露	CVE-2024-6104
2024/12/2	2024/12/4	Linux Kernel 释放后重用漏洞(CVE-2023-6270)	高危	代码执行 拒绝服务	CVE-2023-6270
2024/12/2	2024/12/31	Libuv 信息泄露漏洞 (CVE-2024-24806)	高危	信息泄露 安全特性绕过	CVE-2024-24806
2024/12/2	2024/12/31	Oracle MySQL Client 数据验证不恰当漏洞 (CVE-2024-21247)	低危	代码执行 拒绝服务 信息泄漏	CVE-2024-21247
2024/12/2	2024/12/31	Go JOSE 拒绝服务漏洞 (CVE-2024-28180)	中危	拒绝服务	CVE-2024-28180
2024/12/2	2024/12/31	Google Go 无限循环漏洞 (CVE-2024-24786)	中危	拒绝服务	CVE-2024-24786
2024/11/27	2024/12/6	Zyxel ZLD 防火墙目录遍历漏洞(CVE-2024-11667)	高危	代码执行 信息泄露 拒绝服务	CVE-2024-11667
2024/11/26	2024/12/28	ProjectSend 身份认证绕过漏洞(CVE-2024-11680)	极危	身份认证绕过	CVE-2024-11680
2024/11/20	2024/11/20	Apple 多款产品输入验证错误漏洞 (CVE-2024-44308)	高危	代码执行 安全特性绕过	CVE-2024-44308
2024/11/20	2024/11/20	Apple 多款产品跨站脚本漏洞(CVE-2024-44309)	中危	代码执行	CVE-2024-44309
2024/11/18	2024/11/19	Palo Alto Networks PAN-OS 身份认证绕过漏洞(CVE-2024-0012)	极危	身份认证绕过	CVE-2024-0012
2024/11/18	2024/12/3	Oracle Agile PLM Framework 授权不当漏洞 (CVE-2024-21287)	高危	信息泄露	CVE-2024-21287

公开日期	发现在野利用日期	漏洞名称	危险等级	威胁类型	编号
2024/11/18	2024/12/21	Palo Alto Networks PAN-OS 权限提升漏洞 (CVE-2024-9474)	高危	命令执行	CVE-2024-9474
2024/11/15	2024/12/6	GeoVision 多款产品命令执行漏洞 (CVE-2024-11120)	极危	命令执行	CVE-2024-11120
2024/11/15	2024/12/10	Really Simple Plugins 多款产品身份认证绕过漏洞 (CVE-2024-10924)	极危	身份认证绕过	CVE-2024-10924

注：以上仅展示部分漏洞，点击下载完整列表：

2024年在野利用漏洞列表.csv

（超链接：https://ti.qianxin.com/api/d/c6LajB）

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