工业和信息化部电子第五研究所（中国赛宝实验室） CEPREI

SANGFOR 深信服科技

深信服千里目 Sangfor DeepINSight

2024上半年网络安全漏洞态势报告

2024 MIDYEAR CYBERSECURITY VULNERABILITY TRENDS REPORT

工业和信息化部电子第五研究所软件与系统研究院科研创新部

深信服千里目安全技术中心

报告编写工作组

工业和信息化部电子第五研究所：

陈平、李帅、刘茂珍、余果、顾欣、魏光辉、陈俊名、张宇锖、谢梦珊、李颖琪

深信服科技股份有限公司：

周欣、王振兴、安东冉、禹廷婷、辛佳檬、胡屹松、杜笑宇、刘志远

引言

近年来，网络空间安全的战略地位不断提升，网络安全漏洞作为威胁网络安全的根本性因素之一，其重要性日益凸显。随着新兴技术的不断发展，网络架构日益复杂，系统间的互联互通更加紧密，使得网络安全漏洞的形态和利用手段不断演变。在此背景下，深入了解网络安全漏洞的发展态势，把握其演变规律，对于提升网络安全防护能力、构建安全可信的网络环境具有重要意义。

本报告旨在通过网络安全漏洞总体视角，分析漏洞发展态势与流行利用趋势；根据国内外开源软件漏洞发展现状，分析当前开源软件漏洞威胁态势和治理成效；从实际攻防场景出发，分析漏洞利用新趋势。与此同时，随着人工智能技术的快速发展，也为漏洞利用带了新的变化。本报告围绕以上内容开展分析，希望能够为网络安全行业提供有价值的参考，与全行业共同应对日益严峻的网络安全挑战。

声明

本报告由工业和信息化部电子第五研究所软件与系统研究院和深信服科技股份有限公司联合编写。文中漏洞数据来源于 CNNVD、NVD 等国家级漏洞库和 KEV、OSV、Google Project Zero 项目等行业代表性数据，均明确注明来源，其余数据来源于报告编写团队，目的仅为帮助读者及时了解中国或其他地区漏洞威胁的最新动态和发展，仅供参考。

本报告中所含内容乃一般性信息，不应被视为任何意义上的决策意见或依据，任何编制单位的关联机构、附属机构并不因此构成提供任何专业建议或服务。

摘要

2024 年漏洞发现和披露速度再次加快，2024 年上半年披露漏洞 20548 个，与 23 年同期相比增长 46.16%。预计年底收录漏洞数将突破三万个，这预示着今年的网络安全工作不能放松警惕，需要对安全漏洞的防御和修复投入更多精力。

2024 年全球漏洞利用的产品分布方面，操作系统和浏览器 0day 漏洞数量最多，其中浏览器 0day 漏洞量整体占比呈下降趋势；第三方组件的 0day 漏洞利用量呈上升趋势；针对移动设备的 0day 漏洞利用手段升级，其中接近 50% 被用于执行间谍活动。

2024 年典型攻防场景中，以利用逻辑类 0day 漏洞和传输加密类 0day 漏洞为主，攻击者以此来隐藏攻击特征，比以往攻击更具隐蔽性。其中逻辑类漏洞主要包括业务接口漏洞、认证绕过、账密找回、越权访问等类型。

2024 年典型攻防场景中，漏洞利用方式从战前储备 0day 漏洞逐渐向战前储备和后期新挖掘 0day 为主的方式转变。这一变化与攻防活动周期拉长有较大关系，也与目标范围逐年扩大存在一定关系。

2024 年上半年，披露开源软件漏洞 3618 个，高危及以上占比超 40%。今年仍然需要重点关注由开源软件漏洞引发的软件供应链安全风险。我国应加快开源软件漏洞治理步伐，抓住市场、人才、技术发展机遇与国际化合作趋势，建立“政产学研用”一体化协同共治体系，鼓励开源界先试先行。

2024 年人工智能已成熟落地应用于未知漏洞猎捕和漏洞优先级排序中。在未知漏洞猎捕方面，基于相似度算法和 AI Agent 模式 0day 漏洞归因定性，可以实现自动化 0day 猎捕。在漏洞优先级排序 (VPT) 上，人工智能结合 SSVC 决策树模型，能够快速推理决策出需要优先处置的漏洞。

CONTENTS

目录

安全漏洞总体态势

漏洞公开披露情况

2014 年至 2024 年，我国国家信息安全漏洞库（CNNVD）和美国国家漏洞库（NVD）漏洞收录情况如图 1-1 所示，国内外漏洞库收录漏洞数量的变化趋势保持一致。

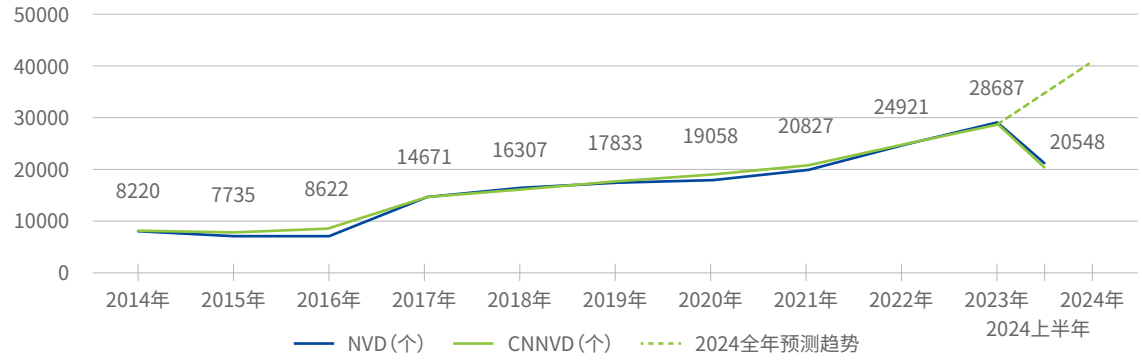

图1-1 近十年漏洞披露情况

2024 年漏洞发现和披露速度再次加快，预测年底收录漏洞数将突破三万个，可见在网络安全工作中，对安全漏洞的防御和修复需要投入更多精力。截至 2024 年 6 月 30 日，CNNVD 共收录 2024 年漏洞信息 20548 条，同比 2023 年漏洞收录数量增加 46.16%，收录速率达到近十年最大值。

由于 2024 年漏洞数量快速增长，美国因预算、流程标准以及合作商等问题导致在 NVD 漏洞库的治理工作上出现了大量堆积工作和时效性不足的问题。自 2024 年 2 月起，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）几乎完全停止了对 NVD 的信息更新。直至 2024 年 5 月，为填补 NVD 信息空白对美国漏洞治理带来的影响，美国网络安全和基础设施安全局（Cybersecurity and Infrastructure Security Agency，CISA）宣布启动“漏洞丰富”（Vulnrichment）计划，在 Github 上开展漏洞分析工作和信息补充工作。

漏洞利用情况

已知被利用漏洞情况

2021 年，美国将已知漏洞利用视为影响其国家网络安全的重大风险，建立已知被利用漏洞（Known Exploited Vulnerabilities，KEV）目录以要求美国联邦机构降低已知利用漏洞的重大风险。至此，KEV 目录也成为了国际上已知被利用的漏洞的权威来源，为各组织提供漏洞修复优先级提供重要指导。KEV 目录的漏洞收录原则有以下三点：漏洞已分配 CVE（Common Vulnerabilities & Exposures）编号、有可靠证据表明该漏洞在真实攻击中已被积极利用、漏洞已有明确的补救措施。

KEV 目录运营效果明显，有效帮助机构识别重要漏洞，加快了漏洞修复速度，平均提速 3.5 倍。截至 2024 年 6 月 30 日 KEV 目录累计已收录漏洞 1126 个。KEV 目录投入运营期间，前两年快速收敛历史漏洞，较好地控制了已知漏洞利用风险。2023 年 9 月，KEV 目录收录漏洞数达到 1000 个，CISA 公布其运营效果称该目录对美国政府 100 多个联邦民用机构的网络安全产生了明显影响，将暴露 45 天或更长时间的可利用漏洞的百分比下降了 72%。从对全球影响效果来看，2024 年 5 月，美国网络安全机构 Bitsight 的研究数据表明，在全球 140 多万个实体（包括公司、学校、地方政府等）对 KEV 所列漏洞的修复时间中位数为 174 天，而非 KEV 所列漏洞的修复时间为 621 天。KEV 目录中列出的漏洞所需的修复时间中位数是非 KEV 漏洞的 3.5 倍。

近十年漏洞利用情况

（一）数量趋势

近 10 年真实漏洞利用数量总体呈现先上升后下降趋势。KEV 目录收录漏洞的 CVE 编号年份进行统计，2021 年漏洞被收录数量最多，达到峰值。2021 年以前漏洞利用总数呈上升趋势，2021 年后呈下降趋势。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，漏洞利用数量于 2021 年开始下降，美国漏洞治理初见成效。

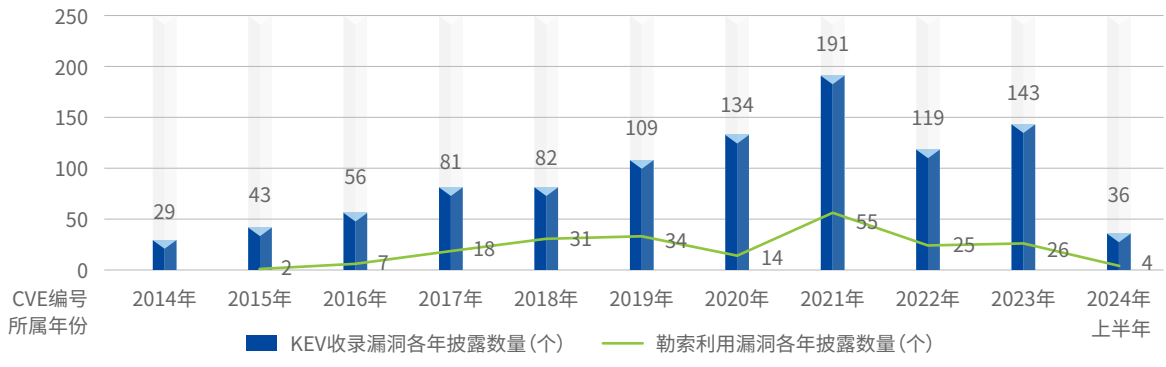

图1-2 KEV目录中近十年漏洞利用情况

截至2024年上半年，KEV目录中已知被勒索软件利用漏洞共228个，其数量变化与整体趋势一致，在2021年达到了峰值。随着全球范围内对勒索软件大型组织的打击，勒索软件整体在漏洞利用上的能力有所减弱，这一变化得益于国际执法机构的协作整治，但勒索软件攻击仍然对企业机构存在着严重威胁。**值得注意的是，随着国际执法机构对勒索组织的打击，对其组织运营产生极大影响，为提高攻击效率勒索组织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。**

2024 年 8 月，美国网络安全和基础设施安全局（Cybersecurity and Infrastructure Security Agency，CISA）与美国联邦调查局（Federal Bureau of Investigation，FBI）和美国国防部网络犯罪中心（DoD Cyber Crime Center，DC3）共同发布了一份联合网络安全公告，揭露近期勒索软件组织的攻击活动，其中重点标记了被利用来执行攻击活动的漏洞，这些漏洞主要用于提供攻击的初始访问权限。包括 Citrix Netscaler（CVE-2019-19781 和 CVE-2023-3519）、F5 BIG-IP（CVE-2022-1388）、Pulse Secure/Ivanti VPN（CVE-2024-21887）以及最近的 PanOS 防火墙（CVE-2024-3400）。其中 2 个 2024 年漏洞在其他攻击活动中也频繁被利用。例如俄罗斯网络安全机构卡巴斯基观测到，Pulse Secure/Ivanti VPN（CVE-2024-21887）在 2024 年第一季度的 APT 攻击活动中利用情况排行第二；PanOS 防火墙（CVE-2024-3400）漏洞在 2024 年第二季度的 APT 攻击活动中利用排行第一。

（二）受影响厂商和产品情况

根据截止到 2024 上半年 KEV 目录收录的 1126 个漏洞分析，受影响厂商排行前十情况如图 1-3 所示。2024 年上半年，KEV 目录收录漏洞 73 个，**Microsoft 和 Google 的漏洞最多，其主要受影响产品分别为 Windows 操作系统和 Chromium V8。**

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 287 个，其次分别为 Apple（75 个）、Cisco（71 个）、Adobe（67 个）、Google（58 个）。**从增长趋势来看，Apple、Ivanti、Google 增长明显，三年间增长 60% 以上。**而 Adobe、Oracle、Apache、D-Link 等近年来被利用漏洞情况有所缓解，其 CVE 编号在 2021 年及以前的漏洞被利用情况相对严重。

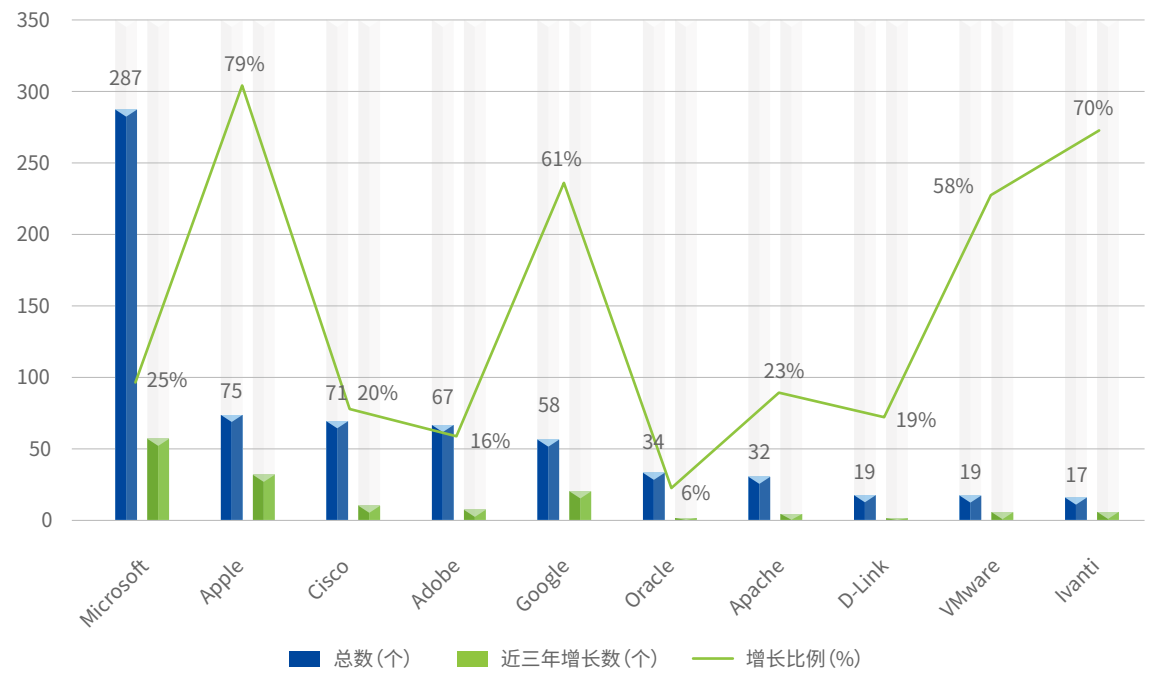

图1-3 影响厂商排行

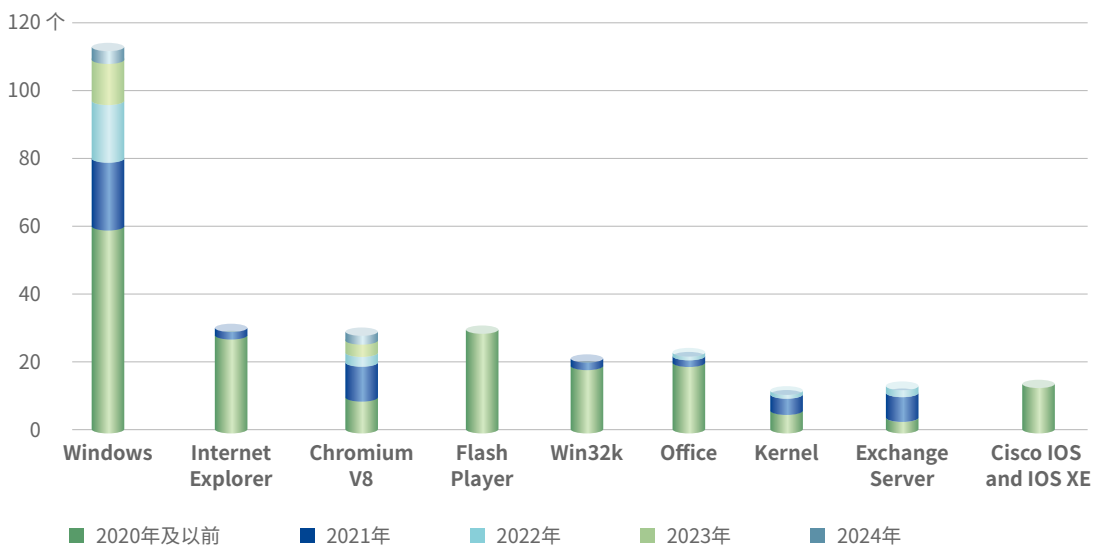

图1-4 影响产品分布

从影响产品情况来看，如图 1-4 所示，在 2021 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。2024 年上半年，根据深信服千里目安全技术中心监测发现，受影响最大的产品仍旧是操作系统和浏览器。

Microsoft 的 Windows 操作系统已知被利用漏洞最多，且近几年来保持稳定增长趋势。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 2021 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。

随着主流浏览器使用情况的转变，漏洞利用重心也从 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 2021 年后未出现新的被利用漏洞。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。

0day漏洞利用情况

全球视角捕获0day利用情况

根据谷歌捕获 0day 漏洞利用情况来看，2024 年上半年发现 0day 漏洞数量与 2022 年和 2023 年同比均有不同程度的减少。根据 Google Project Zero 项目数据来看，2023 年共有 97 个 0day 被利用，与 2022 年发现的 62 个 0day 相比大幅增加，但仍低于 2021 年 106 个 0day 的历史峰值。对近一年来 0day 漏洞利用情况分析，得出如下几点总结。

01

操作系统和浏览器 0day 漏洞数量最多，其中浏览器 0day 漏洞整体占比下降。从攻击难度和攻击效益来看，浏览器 0day 漏洞攻击实施复杂度低、攻击效益高。而近两年来，所有主流浏览器均采取了新的防御措施，使浏览器漏洞利用难度逐渐增加，所以浏览器 0day 漏洞利用的占比呈下降趋势。

02

第三方组件 0day 漏洞利用越来越多，攻击者倾向利用第三方组件漏洞进行供应链攻击。在近一年的 0day 漏洞利用中，针对第三方组件的利用比起往年更加频繁，主要体现在浏览器组件中，这些漏洞几乎同时会影响所有主流浏览器，如 Chrome、Safari、Firefox。Skia 是 Google 开发的一个开源 2D 图形库，被广泛用于 Chrome、ChromeOS、Android 和 Firefox 等多个项目，在 2023 年发现其存在 2 个 0day 漏洞（CVE-2023-2136 和 CVE-2023- 6345）在野利用情况。

03

针对移动设备的 0day 漏洞利用手段升级，近一半被用于执行间谍活动。具体表现为针对移动终端设备制作间谍软件形成商业化，向世界各地的政府出售尖端技术以帮助其窃取目标数据。近年来，在多起活动中披露通过移动设备的间谍软件窃取国家政府人员重要数据，主要归因于移动设备操作系统和浏览器更新速度慢，漏洞影响力持久，使得攻击者可持续潜伏。

国内视角捕获0day利用情况

聚焦我国漏洞利用场景，2024 年上半年报告编写团队捕获真实利用 0day 漏洞 100 多个，其中 SQL 注入漏洞最多，占比 50%，其次为文件上传、信息泄露和反序列化漏洞等。2023 年猎捕到 300 多个 Web 场景下的 0day 漏洞利用，其中 50% 以上出现在实战攻防演练场景中。随着攻防常态化，将会有越来越多的 0day 被利用在网络攻击中，对于 0day 漏洞的发现与防护迫在眉睫。

0day 漏洞在野利用平均周期为 37 天。根据报告编写团队监测发现，2024 年上半年从发现 0day 漏洞利用到实际漏洞披露时间平均为 37 天。而这些在野利用 0day 漏洞的平均修复时间约为 30.6 天。根据全球领先的云安全和漏洞管理提供商 Qualys 的研究报告显示，Chrome 和 Windows 相关高可利用漏洞的平均修复时间为 17.4 天，有效补丁率为 82.9%。Windows 和 Chrome 的修补速度和频率是其他应用程序的两倍。

01

通过对已修复漏洞的绕过或者修复不彻底漏洞的变体利用形成新的 0day 漏洞现象在近几年屡次出现。根据报告编写团队监测数据，在 2023 年的 0day 漏洞中发现有 7 个变体漏洞利用情况，其主要由于漏洞根本问题没有得到解决，使攻击者能够通过新的路径触发原始漏洞。在 2022 年 0day 漏洞中也有 7 个变体漏洞利用，其中有 4 个是 2021 年发现 0day 漏洞的变体。可见无论是 0day 漏洞的发现还是修复，都存在很大的提升空间，需要产品提供者对补丁管理和 0day 漏洞的发现采取更为积极的态度。

02

随着 AI 技术的发展，漏洞利用工具化进一步加速。根据报告编写团队研究发现，部分 0day 漏洞会在披露的当天迎来大规模利用，并且攻击效率不断提高。根据全球领先的云安全和漏洞管理提供商 Qualys 的研究数据表明，75% 的漏洞在披露后的 19 天内会被利用。通过快速利用刚刚披露的 0day 漏洞，在漏洞未修复的时间窗口内，利用自动化工具发起大规模攻击，从而拉开攻击与漏洞修复的时间差，取得更好的攻击效果，同时挖掘成本也更低。2024 年 5 月，知名美国 CDN 服务商 Cloudflare 观察发现最快在漏洞披露 22 分钟后出现利用，这使得防御者几乎没有时间修复。

03

攻防场景漏洞利用趋势

攻防场景下的0day利用情况

2024 年典型攻防场景中，主要通过利用逻辑类 0day 漏洞和传输加密类 0day 漏洞隐藏攻击特征，使攻击比以往更具有隐蔽性。

对比往年，2024 年攻防场景中 0day 漏洞利用更具有隐蔽性。攻防场景中，攻击者越来越多地使用逻辑漏洞进行攻击，包括业务接口漏洞、认证绕过、账密找回、越权访问等，逻辑漏洞利用相对隐蔽，不易被发现，利用难度较低，为攻击者提供了更多操作空间。此外，攻防场景中攻击者还会利用一些默认对传输加密的漏洞，例如某 OA 软件在进行数据序列化过程中会使用 AES 加密、GZIP 编码、Base64 编码等多种编码和加密的方式，这会隐藏原始的攻击特征，让安全设备更难发现攻击，以达到攻击者隐蔽攻击的目的。

2024 年典型攻防场景中，漏洞利用方式从战前储备 0day 漏洞逐渐向战前储备和后期新挖掘 0day 为主的方式转变。

对比往年攻防场景，今年更多的是针对特定目标进行定向挖掘新漏洞，这与攻防活动周期拉长有较大关系。攻防活动中后期，利用储备 0day 漏洞已无法有效攻击目标，攻击者会根据目标系统定向挖掘其漏洞，或者通过在攻击目标相关的供应链中寻找突破口进行渗透，获取供应商的源代码并从中挖掘漏洞进行攻击，进而拿下目标站点系统权限，以达到更佳的攻击效果。

2024 年典型攻防场景中的 0day 漏洞以获取系统权限为主，OA、ERP、CRM、EHR、报表等商业办公系统类 0day 漏洞利用频率最高。

表 2-1 为 2024 年攻防场景重点 0day 漏洞，可以看出，漏洞类型主要以代码执行漏洞、任意文件上传漏洞、反序列化漏洞和 SQL 注入漏洞为主，攻防场景中这几种类型的漏洞是攻击者常用来获取系统权限的手段。OA、ERP、CRM、EHR、报表等商业办公系统类的 0day 漏洞依旧是使用频率最高的漏洞，由于其软件使用的广泛性，而且大多数对互联网开放，因此风险暴露面较大。但是基于往年攻防场景经验，商业办公系统供应商一般会进行大规模的安全漏洞修复，并发布安全补丁通过内部的服务流程为用户进行安全补丁更新，这导致攻击者难以利用历史漏洞，需要挖掘新的 0day 漏洞进行攻击。同时，在攻防活动期间漏洞响应的速度会加快，部分软件厂商 0day 漏洞信息披露到修复的周期在 1-2 天。

表2-1 2024年攻防场景重点0day漏洞的相关情况

组件名称	漏洞类型	影响范围(资产测绘)
某报表系统	代码注入漏洞	★★★★★
某报表系统	代码注入漏洞	★★★★★
某企业管理软件	反序列化漏洞	★★★★
某企业管理软件	反序列化漏洞	★★★★
某 OA	代码注入漏洞	★★★★
某 OA	代码注入漏洞	★★★★
某 OA	代码注入漏洞	★★★★
某 OA	代码注入漏洞	★★★★
某电子文档安全管理系统	SQL注入漏洞	★★★★
某采购管理系统SRM	代码注入漏洞	★★★★
某 OA	文件上传漏洞	★★★★
某中间件	反序列化漏洞	★★★★
某企业管理软件	反序列化漏洞	★★★★
某印章管理系统	文件上传漏洞	★★★
某 OA	SQL注入漏洞	★★★
某印章管理系统	代码注入漏洞	★★★
某项目管理系统	代码注入漏洞	★★★
某云服务产品	远程代码执行漏洞	★★★
某人力资源管理系统	反序列化漏洞	★★★

攻防场景下的Nday利用情况

典型攻防场景中使用的 Nday 漏洞主要集中在使用范围广泛的组件中。

对近几年攻防场景中爆出的漏洞进行盘点，观察到攻防场景中使用的 Nday 漏洞多分布在使用范围广泛的组件中，如 docker、Nacos、Oracle WebLogic 和 JBOSS 等组件。表 2-2 为近年来攻场景中重点 Nday 漏洞组件、漏洞类型和影响范围的情况。（本文主要根据资产测绘情况来确定影响范围）从公网资产来看，大多数重点 Nday 漏洞所属组件的公网资产数量是非常大的，由于组件覆盖率高，且部分漏洞可以通杀多个版本，利用这些 Nday 漏洞对于通用目标的攻击非常高效。

表2-2 近年来攻防场景重点Nday漏洞的相关情况

组件名称	漏洞类型	影响范围（资产测绘）
docker	未授权访问漏洞	★★★★★
Nacos	未授权访问漏洞	★★★★★
Oracle WebLogic	远程代码执行漏洞	★★★★★
JBOSS	远程代码执行漏洞	★★★★★
OA	远程代码执行漏洞	★★★★
Confluence	远程代码执行漏洞	★★★★
Confluence	未授权访问漏洞	★★★★
Redis	未授权访问漏洞	★★★★
Jenkins	远程代码执行漏洞	★★★★
Gitlab	远程代码执行漏洞	★★★★
Elasticsearch	未授权访问漏洞	★★★
Memcached	未授权访问漏洞	★★★
Apache Flink	未授权访问漏洞	★★★
Netlogon	权限提升漏洞	★★★
Active Directory Domain Services	权限提升漏洞	★★★

典型攻防场景中 Nday 漏洞工具化十分常见。

从近年来的攻防场景来看，漏洞利用仍然是攻击方入侵的重要手段，利用重点 Nday 漏洞，将 Nday 漏洞进行工具化已屡见不鲜，对于高可利用漏洞进行工具封装，可实现一个漏洞通杀所有版本。一体化的攻击工具可以实现一键快速打点，自动实现资产指纹收集、漏洞自动检测、利用以及获取权限等功能。此外，攻击方会开发自动化平台，集成漏洞工具，攻击人员通过平台接口协同配合，以加快攻击过程，形成完整的自动化攻击链。

典型攻防场景中 Nday 漏洞组合利用攻击效果更加显著。

通过多个漏洞组合利用，以达到比单个漏洞更深入、更有效的攻击效果。这种利用方式通常用于目标系统的安全措施较为严密，单一漏洞难以突破防御时，漏洞组合利用可以发挥更佳的效果，这与近几年攻防整体水平的提高有较大关系。越来越多的业务系统针对历史漏洞的修复是通过添加登录授权的方式，将原来前台可访问的接口，控制在后台访问，收敛了业务的暴露面，这也导致前台的代码执行漏洞越来越少，很多需要先进入后台才能利用。今年的攻防场景中，攻击者利用 Nacos 漏洞获得业务系统数据库密码，进一步登录业务系统后台，这也导致原本收敛到后台的历史漏洞死灰复燃，再一次暴露在攻击者的面前，通过利用后台漏洞，攻击者可以获得业务系统权限。

攻防场景下的漏洞利用路径

2024 年典型攻防场景中，攻击者通过供应商源代码审计等方式挖掘其漏洞进而进行供应链攻击，扩大攻击面。面对无法直接突破的目标，或者希望扩大攻击面影响范围时，供应链攻击是一个很好的选择。例如社会服务相关部门的站点往往拥有较好的安全防御体系，直接攻击难以突破。但是相关业务下会拥有诸多服务平台，可以从相关的供应链公司中寻找突破口进行渗透，获取供应商的源代码并从中挖掘出任意密码用户重置、管理员密码泄漏、前台 RCE 等漏洞，进而拿下站点的权限。另外，如果目标系统的供应商可以确定，通过目标系统的指纹、公开招标信息等线索，可以搜索到供应商旗下相关系统。某些供应商往往会存在一个统一的云平台管理系统或者数据管理平台，对多个系统进行运维和管理。一旦爆破出用户名密码进入到系统后台，就可能拥有公司旗下多个系统的默认管理员密码，再去目标系统登陆就可成功进入后台。供应链攻击往往隐蔽性较强，在真实的 APT 攻击场景下，可能很早就潜伏于目标系统的第三方资源开发中，在更新版本中植入恶意代码，悄无声息地入侵目标系统。

01

2024 年典型攻防场景中，攻击者通过加密、混淆等方式改造攻击流量以绕过安全设备，边界安全对抗再次升级。在初始访问阶段，针对安全设备的攻防对抗更加激烈。攻击者通过加密、混淆、填充垃圾字符等方式改造攻击流量，从而绕过安全设备的防护策略，突破边界安全防线。从 2024 年攻防场景来看，攻击者对于文件上传漏洞中构造的恶意 Webshell 进行混淆和通信加密的操作，这会导致针对原始 Webshell 上传特征和通信流量特征进行防护的安全设备无法匹配到已经被攻击者破坏的攻击特征，造成防护能力失效。此外针对代码注入漏洞的垃圾字符填充，也会绕过一些有检测长度限制的安全设备。

02

2024 年典型攻防场景中，漏洞攻击逐渐聚焦于云管平台、堡垒机、域控等集权设备。企业内网中的集权设备通常承担着关键的安全管理和集群控制等关键功能，因此成为攻击者的主要目标。例如，攻击者通过突破网络边界后会进行横向渗透，通过端口扫描、指纹特征、信息收集等方式寻找企业内网中的云管平台、堡垒机、域控等集权类设备。在定位到集权类设备后，攻击者往往会利用 0day 漏洞、1day 漏洞等攻击手段获取集权设备的权限，从而获取企业中大量重要业务系统服务器和关键人员办公终端的权限。

03

开源软件漏洞态势

开源软件漏洞威胁态势

近年来，开源软件漏洞数量整体呈增长趋势，2024 年上半年统计数据显示，高危及以上漏洞占比超过 40%，开源软件作为软件供应链的重要组成部分，一旦爆发严重漏洞将对整个软件供应链带来极大安全风险。开源漏洞数据库（Open Source Vulnerability，OSV）数据显示，近 10 年披露的开源软件漏洞总计 51858 个，从十年增长率来看，整体呈增长趋势，历年高危及以上漏洞占比均超 40%。漏洞数量逐年增长和高危以上漏洞占比居高，与近年来开源项目的增多和全球开源软件大事件的频发存在一定关系。

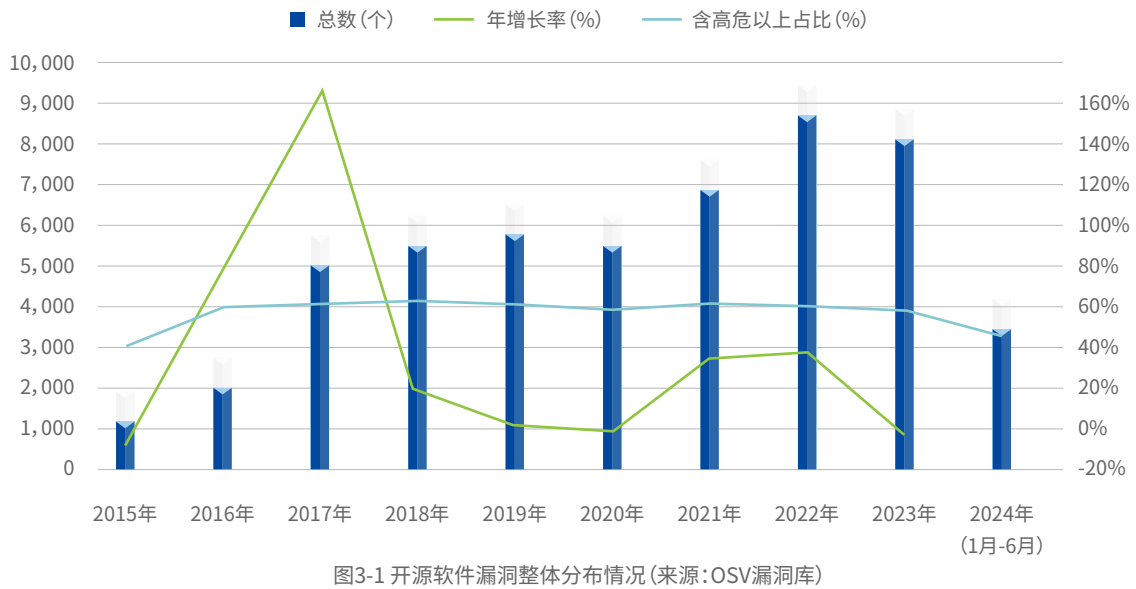

图3-1 开源软件漏洞整体分布情况（来源：OSV漏洞库）

开源软件漏洞最主要缺陷类型为 CWE-79，近一年来，CWE-89 上升最快，目前排名第二。根据对 OSV 漏洞数据库数据统计分析，发现缺陷类型为 CWE-79 的漏洞数量最多，占近 10 年漏洞总数的 13%。近一年多以来，缺陷类型为 CWE-89 的漏洞上升最快，新增漏洞 418 个。

表3-1 开源软件漏洞 TOP10 CWE 缺陷类型总体情况（来源：OSV漏洞库）

CWE编号	中文名称	漏洞总数
CWE-79	跨站脚本	6539
CWE-119	缓冲区错误	2901
CWE-787	越界写入	2600
CWE-20	输入验证不恰当	2374
CWE-125	越界读取	1976
CWE-416	释放后重用	1727
CWE-200	信息暴露	1513
CWE-22	路径遍历	1486
CWE-89	SQL注入	1409
CWE-476	空指针解引用	1383

表3-2 2023年第一季度-2024第二季度开源软件漏洞 TOP10 CWE 缺陷类型（来源：OSV漏洞库）

CWE编号	中文名称	2023 Q1 -2024 Q2 漏洞数量
CWE-79	跨站脚本	1455
CWE-89	SQL注入	418
CWE-416	释放后重用	372
CWE-787	越界写入	351
CWE-22	路径遍历	305
CWE-352	跨站请求伪造（CSRF）	248
CWE-476	空指针解引用	189
CWE-400	未加控制的资源消耗	186
CWE-125	跨界内存读	183
CWE-20	输入验证不恰当	166

Maven 仓库漏洞数量现居榜首，2022 年主流生态仓漏洞均有明显增加，2024 年增速放缓。根据 GitHub Advisory Database 数据显示，对 Github 已审核的 19525 个开源软件漏洞进行分析，发现 Maven 仓库漏洞数量最多，总计 4994 个，2022 年各仓库漏洞增速最快，环比增长 221%。

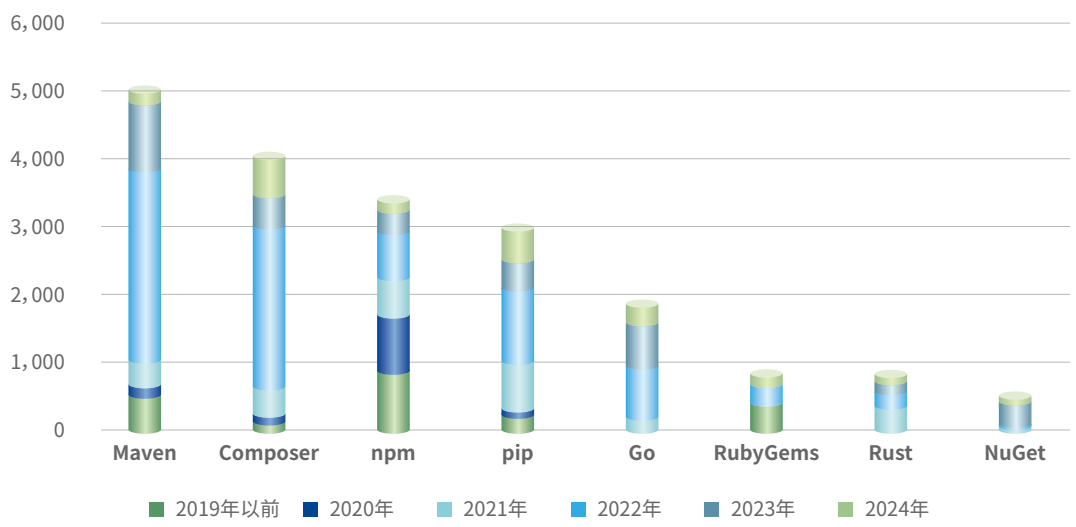

图3-2 开源软件主流仓库漏洞按时间分布情况（来源：GitHub Advisory Database）

在 Github 漏洞库已审核漏洞中，高危及以上漏洞占比 50%，暴露了当前开源软件在安全性方面仍存在风险，同时也反映了软件供应链安全问题的严重性。根据 GitHub Advisory Database 数据显示，截止 2024 年 7 月 15 日，Github 漏洞库已审核漏洞 19525 个，严重漏洞占比 15%，高危漏洞占比 35%。（GitHub Security Advisories 是一个专注于开源领域通用漏洞披露的数据库，是开源软件漏洞领域最具权威的漏洞库之一，基于通用漏洞披露（CVE）列表而构建。）

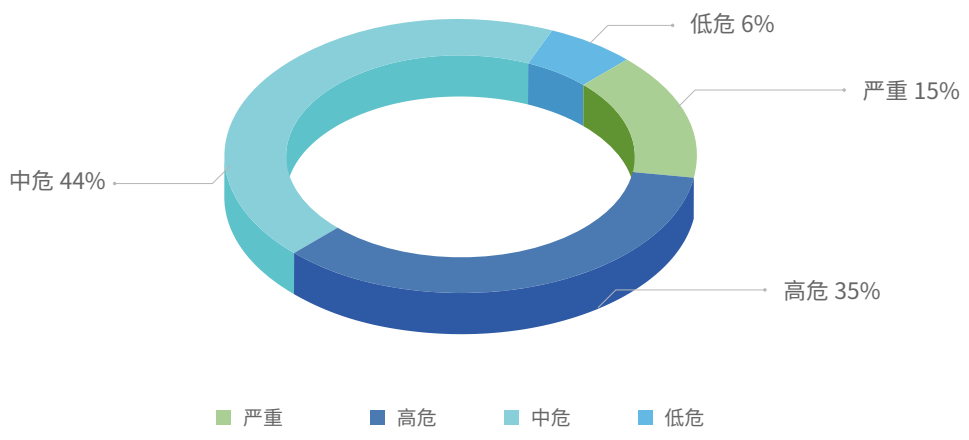

图3-3 开源软件漏洞危害占比（来源：GitHub Advisory Database）

开源软件漏洞的影响

01

开源软件漏洞传播链长，危害性沿链逐级放大。复用开源软件的情况在现代软件开发中愈发普遍，软件供应链也随之复杂多元。开源软件属于软件开发原料，攻击者可以通过软件供应链的上下游关系，利用开源软件对下游软件发起裂变式恶意攻击。CNCERT《开源软件供应链安全风险研究报告》调查结果显示，选取 17，570 个含漏洞的开源文件中，超 80% 的文件可在开源项目中找到同源文件。该报告的另一调查结果显示，开源组件漏洞一级传播（直接依赖）影响范围扩大 125 倍，二级传播（间接依赖）影响范围扩大 173 倍。

02

开源软件漏洞影响范围大，持续时间长。2021 年曝出的 Log4j2 安全漏洞事件，是典型的软件供应链安全漏洞事件，Apache 安全团队公布了受影响软件项目列表，涉及 Cloudflare、iCloud 等多个国际知名商业服务，影响了 93% 的企业云环境。据统计，35000+ 个开源软件 Java 组件依赖于 Log4j2，意味着超过 8% 的软件包里至少有一个版本会受此漏洞影响，可见该漏洞影响范围之大。美国网络安全审查委员会首份报告指出，Log4j2 漏洞要十余年才能修完，将在未来十年甚至更长时间持续引发风险，持续时间之长可见一斑。

03

开源软件漏洞维护成本大，责任落实难。主要受以下因素影响：开源软件通常依赖于社区的支持来发现和修复漏洞，社区的规模和活跃程度会影响漏洞修复的速度和质量，然而社区的规模及活跃度往往参差不齐；开源软件供应关系网络错综复杂，增加了发现和修复漏洞的难度，修复漏洞往往需要更多的时间和资源；开源软件通常面临大量的漏洞报告和修复请求，管理这些漏洞并及时响应需要专门的漏洞管理流程和工具，增加了开源软件漏洞的维护成本。开源软件漏洞责任落实困难，开源软件开发者群体分散，导致开源软件漏洞的责任界定和追溯变得复杂；开源项目通常依赖于捐赠，可能由于资金和资源的限制导致漏洞修复延迟或不完善；在某些国家和地区，缺乏明确法律框架，从而影响了漏洞的及时修复和责任的追究。

国外开源软件漏洞治理工作与成效

开源政策、法律纷纷出台，引导开源健康可持续发展之路。2023 年，美国发布《2023 国家网络安全战略》，旨在建立一个“可防御、有韧性的数字生态系统”，CISA 发布了一份开源软件安全路线图，重视开源软件漏洞“连锁”效应和供应链“投毒”等特有风险及应对措施；欧盟《网络安全弹性法案》进入立法程序，采取了分层方法来处理开源软件的安全问题，并明确数字产品制造商、进口商、分销商等相关方漏洞治理责任。

01

开源软件漏洞治理标准、工具大量涌现，加速搭建开源治理基底。2022 年，Linux 基金会主办的开源软件安全联盟 OpenSSF 发布了开源软件安全的系列指南，包括《评估开源软件的简明指南》、《安全研究人员与开源软件项目协同漏洞披露 (CVD) 指南》、《开发更安全软件的简明指南》、《NPM 最佳实践指南》，提供了开源软件开发、使用、漏洞批量、包管理等方面的最佳安全实践。2023 年，OpenSSF 发布了数字签名 Sigstore、恶意包检测仓 Malicious package repository、安全仪表盘 Scorecard 等系列工具，应用于 GitHub 平台，为上万个开源软件项目提供代码安全审计、检测、评估等服务。

02

开源软件漏洞激励机制、赏金计划，激发了广大安全研究员挖掘开源软件漏洞的热情。2022 年，谷歌推出了专门针对开源软件的漏洞赏金计划（OSS VRP），这是首批特定于开源的漏洞计划之一，重点关注谷歌软件和存储库设置，该计划在 2023 年向来自 68 个国家的 632 名研究人员支付了 1000 万美元。

03

我国开源软件漏洞治理挑战与机遇

（一）两大挑战

一是国内外漏洞信息共享机制尚未完全建立

国内尚未发布针对开源软件漏洞协同处置与披露的规范指南，目前只有少部分大型开源项目建立了开源软件漏洞报送与处置流程，与其他上游社区存在一定的漏洞感知时间延迟。

二是国内软件安全开发能力与治理动力不足

国内开源软件漏洞治理的激励政策、激励计划仍然较少，难以有效持续吸引高水平安全人才。高校对开源软件安全人才的培养尚未形成规模化、系统化和体系化。企业在实施软件安全开发过程中面临诸多困难，如法律法规在软件安全上的落地执行、团队成员缺乏足够的安全意识、开源安全复合型人才紧缺、软件安全风险实时变化等。

（二）四大机遇

一是顺应国际化合作趋势

开源软件由全球开发者共创、共享、共治，汇聚全球开发者和研究者的智慧，顺应国际化合作趋势，协作发现和修复漏洞，上下游共享漏洞信息和资源，建立统一的漏洞披露标准和最佳实践。在全球化趋势之中，提高全球开源软件安全性，也意味着提升我国开源软件安全性。2023 年，国内开源领域唯一的国家级基金会——开放原子开源基金会发布了开源软件漏洞共享平台及安全奖励计划，激励国内白帽积极挖掘开源软件漏洞，与开源项目方、基金会安全专家协同开展漏洞处置，提高开源软件的安全性。

二是符合国内数字化建设发展的安全内需

开源软件已成为数字化基础设施的重要组成部分，在云计算、大数据、人工智能等领域被广泛应用。开源软件在为各行业企业数字化转型提供便利的同时也带来了严峻的安全风险，智能制造、电力、能源、汽车等重要行业领域应加强开源软件漏洞治理，尽量避免 Log4j2 类似安全漏洞事件的发生。

三是开源人才新生力量持续注入

国内拥有超过 1200 万的开源开发者和高校毕业生已加入开源生态圈，积极开展开源软件开发、维护等工作，开源人才的持续孵化，有望推动新一轮全球开源发展升级。

四是人工智能大模型技术兴起，推动漏洞治理工作自动化、智能化和高效化

人工智能大模型技术拥有强大的数据处理和分析能力，通过模型训练和指令微调，能够自动化开展提供代码安全审计、漏洞检测、漏洞挖掘，提供漏洞修复建议，极大降低漏挖技术门槛，提升工作效率。

人工智能技术对安全漏洞的影响

人工智能技术发展过程对安全漏洞利用的影响

随着人工智能技术的日益成熟与普及，在为社会生产生活提供一系列便利的同时，也为网络空间的安全格局带来了全新的挑战，导致了一系列的安全漏洞威胁。从早期的技术积累发展到决策式小模型，再到如今生成式大模型的飞速发展，人工智能的核心逐渐转向了对更大规模模型训练和更强大的计算能力的需求。将 Agent 模式与生成式大模型相结合，将极大地提升模型的自主性，推动 AI 应用从简单的被动响应向积极的主动引导转变，实现质的飞跃。

早期以 AI 决策式小模型或工具参与自动化漏洞挖掘、漏洞利用等过程，提高黑客攻击效率。

此阶段主要利用 AI 决策式小模型或工具开展安全漏洞攻击的方式，将一些重复且耗时的操作自动化、智能化，从而达到提高效率、降低成本等目的。在这种模式下，人工智能可以替代完成部分人力工作。

在漏洞挖掘领域，攻击者能够通过 AI 工具自动化深入挖掘软件或系统的内部缺陷，从而识别潜在安全漏洞。2013 年，美国国防高级研究计划局（DARPA）启动了 CGC 项目，目标是实现漏洞挖掘、分析、利用和修复的全自动化流程，以构建一个具备自动化攻防能力的高性能网络推理系统。在 2014 至 2016 年间，DARPA 举办了“网络超级挑战赛”，旨在测试是否有可能开发出能够发现、验证和修补软件漏洞的人工智能系统。2017 年起，中国也开始举办同类型的自动化攻防竞赛 RHG，其内容涵盖了自动化漏洞挖掘和自动化漏洞利用两大方向。

在漏洞利用方面，人工智能可以被用来自动识别和利用软件中的安全漏洞，从而极大提高黑客的攻击效率。人工智能技术在不同漏洞类型的自动化利用中都发挥了重要作用。例如 FUZE 就是基于内核 UAF（使用后释放）漏洞的自动化漏洞利用生成方案，FUZE 利用机器学习辅助漏洞发现，通过深度学习优化符号执行的过程，以分析内核中漏洞点上下文的行为，生成漏洞 POC。在确认利用环境后，FUZE 会计算堆喷数据，从而实现漏洞利用。

AI 生成式大模型兴起以来，其在辅助黑客实施与安全漏洞相关的恶意行为方面的潜力引起了关注，这在一定程度上降低了黑客攻击的技术门槛。

自 2022 年底 OpenAI 发布 ChatGPT 以来，人工智能在为人类带来便利的同时，也为网络攻击者提供了新的攻击思路。生成式大模型模式的介入，使得初级黑客可以借助 AI 大模型，批量生产出攻击脚本、制作黑客工具。随着大模型在网络攻防领域的应用日益扩大，安全研究者们开始越来越关注大模型在网络安全漏洞利用方面的能力。

在漏洞利用领域，2024 年 4 月发布的《LLM Agents can Autonomously Exploit One-day Vulnerabilities》论文对大模型自主利用 1day 漏洞的能力进行了研究，研究表明，GPT-4 能够在给定 CVE 描述的情况下，自主利用其中 87% 的漏洞。即使在处理未知漏洞时，GPT-4 仍然保持了高达 82% 的漏洞利用成功率。在验证人类有效性方面，美国加州大学艾尔文分校所出的一项研究显示，AI 已能够应对点击类、拖拽类、图片选择类等市面上各种类型的验证码，最快甚至能在 1.4 秒内通过这些验证。在大模型恶意利用方面，由于现有大模型都对存在黑客行为的输出进行了一定的限制，网络犯罪分子开始在地下论坛推出专门用于恶意目的的恶意大模型，提供如查找安全漏洞、利用安全漏洞、生成安全漏洞等非法服务。

未来 AI 大模型将以 AI Agent 模式开启人工智能自主利用漏洞完成攻击的新型攻击范式。

随着人工智能技术的不断进步，我们正迈向可以由一个人工智能完全替代人类黑客执行攻击任务的时代。在这个时代，**融合“AI Agent”的 AI 大模型不仅能够自动识别和分析潜在的漏洞，还能自主决策并执行复杂的攻击策略，从而实现对安全漏洞的全面利用。**未来，高度自主化、智能化的“AI Agent”大模型将进一步降低对人类干预的需求，提高攻击的效率与隐蔽性，给网络安全带来前所未有的挑战。未来，超高水平的攻击者很有可能借助大模型技术，大幅提升 0day 攻击的生产数量和质量，甚至可能积攒核弹级的 0day 攻击潮，突破即有安全漏洞防御体系。

人工智能产品自身存在的安全漏洞风险

AI 大模型发展至今，其广泛应用正推动着各行各业信息系统的智能化转型。随着应用深度和广度的不断扩展，AI 大模型必将发展成为基础信息设施的智能化底座，但与此同时，其中涉及的各种算法、架构、API 等也可能带来一系列潜在安全漏洞风险。

2023 年 10 月，OWASP 发布了大语言模型（LLM）应用程序的十大安全漏洞清单《OWASP TOP 10 for LLM Applications》，清单内容如表 4-1 所示。

表4-1 OWASP TOP 10 for LLM Applications

序号	OWASP TOP 10 for LLM Applications 清单	中文名称
1	LLM01: Prompt Injection	提示注入
2	LLM02: Insecure Output Handling	不安全的输出处理
3	LLM03: Training Data Poisoning	训练数据中毒
4	LLM04: Model Denial of Service	模型拒绝服务
5	LLM05: Supply Chain Vulnerabilities	供应链漏洞
6	LLM06: Sensitive Information Disclosure	敏感信息泄露
7	LLM07: Insecure Plugin Design	不安全的插件设计
8	LLM08: Excessive Agency	过度代理
9	LLM09: Overreliance	过度依赖
10	LLM10: Model Theft	模型盗窃

OWASP 对大语言模型应用程序架构中存在的 TOP 10 安全漏洞进行了详细阐述，主要包括 LLM 应用服务窗口、LLM 生产服务、插件 / 扩展、下游服务、训练数据集和处理、外部数据源等环节。整个大模型主要以 LLM 生产服务模块为主，通过训练数据集不断优化性能，并通过 LLM 应用服务窗口和插件 / 扩展的形式与外界交互，如图 4-1 所示。

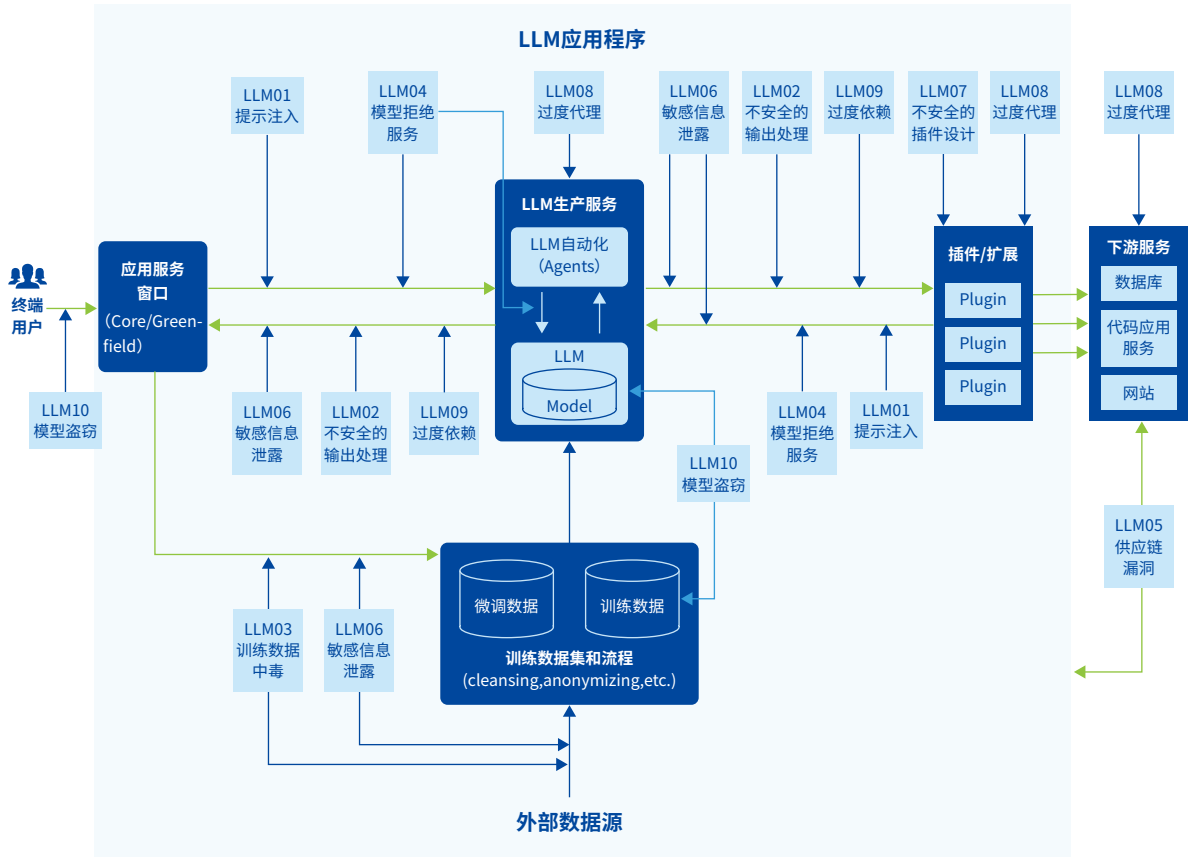

图4-1 OWASP TOP 10 for LLM Applications 与大模型应用程序架构图（来源：OWASP）

《OWASP TOP 10 for LLM Applications》清单整体内容可归结为大模型应用安全、数据安全、系统安全和人员安全风险等问题。大模型安全中涉及安全漏洞风险的问题主要有模型平台安全、供应链安全、信息和内容安全。根据对图 4-1 中大模型应用程序架构图的分析，在**大模型最核心的生产服务模块，存在自身与外部交互的输入输出环节，安全风险最为显著，最频繁出现包括敏感信息泄露、输入输出安全验证、访问控制和权限管控等问题。**这些都可能成为攻击者的攻击入口，对目标系统开展网络攻击活动。结合 AI 大模型应用程序的架构与实际攻击场景，以下将探讨 TOP 10 安全漏洞风险在各环节中的具体攻击情境。

LLM01：Prompt Injection（提示注入）：该漏洞主要出现在大模型服务接口和应用插件在与大模型生产模块的数据交互环节，通过“越狱”（直接）或构造恶意输入（间接）方式与大模型交互，利用大模型进行非法操作，可能导致敏感信息泄露、未授权访问等漏洞出现。

LLM02：Insecure Output Handling（不安全的输出处理）：大模型生产模块输出内容并传递时未经充分的验证和处理，将生成的恶意内容传递给下游系统组件，包括大模型应用服务接口和下游系统组件与大模型的传输接口处，可能导致 XSS、CSRF、权限提升或远程代码执行等漏洞出现。

LLM03：Training Data Poisoning（训练数据中毒）：该漏洞主要存在于训练数据集合模块，由于从外部输入内容或训练数据源被恶意投递不安全的数据，导致大模型训练数据被篡改生成错误内容，甚至可以通过篡改数据引入安全漏洞来破坏大模型安全性，从而达到攻击目的。

LLM04：Model Denial of Service（模型拒绝服务）：与 DDOS 攻击相似，以消耗极高资源的方法对大模型应用进行恶意交互，使大模型服务受到干扰甚至崩溃，具体出现环节包括大模应服务接口与大模型生产模块之间，以及在大模型生产模块中的 LLM Automation 与核心处理模型之间。攻击构造手法包括对大模型上下文窗口的输入溢出、上下文反复扩展递归等等，造成大模型崩溃。

LLM05：Supply Chain Vulnerabilities（供应链漏洞）：在整个大模型的应用程序架构中，使用的第三方模型、插件或数据源都可能存在供应链漏洞从而导致整个大模型出现安全问题，具体可表现为第三方组件漏洞、训练数据源中毒、第三个插件的安全问题。根据 OWASP 提供的案例来看，Open AI 第一次数据泄露就是由攻击者利用存在漏洞的 Python 库导致。

LLM06：Sensitive Information Disclosure（敏感信息泄露）：可能因为输出校验和过滤机制不完善、训练数据过程中出现未脱敏以及模型学习上判断上的误差等问题，导致 LLM 在输出中泄露敏感信息、私有算法或机密信息等，出现未经授权访问及隐私泄露等现象。此问题贯穿于大模型应用架构的每个数据流转环节，是出现次数最高的安全漏洞。

LLM07：Insecure Plugin Design（不安全的插件设计）：大模型与下游应用服务交互的插件往往是在集成平台自动驱动，其本身具备一定的权限。然而其在自主设计可能出现访问控制不足的情况，导致攻击者恶意请求插件，从而引发远程代码执行、数据泄露、权限提升等安全问题。

LLM08：Excessive Agency（过度代理）：在大模型的使用过程中，通常会赋予大模型生产模块对系统一定程度的操作权限以具备一定的自主能力。在这个过程中授予大模型过度的调度功能和权限将可能被攻击者恶意利用执行未授权的攻击行为，甚至通过大模型作为跳板，对下游系统漏洞进行利用或进行远程命令执行操作等。

LLM09：Overreliance（过度依赖）：过度依赖主要指人为因素，当人们对 LLM 生成的内容过度信任，未进行适当的验证，可能导致传递错误信息或带来安全漏洞等。

LLM10：Model Theft（模型盗窃）：大模型本身可能是企业核心资源，承载了大量数据和计算资源。攻击者可能在经济利益、恶意竞争、学术窃取等动机的驱使下，利用未授权访问漏洞访问大模型存储库、利用侧信道攻击获取模型权重和架构等方式进行模型窃取。

人工智能技术为安全漏洞防御力提升赋能

人工智能技术，这把现代科技的双刃剑，在降低黑客攻击门槛的同时，也为加固网络安全防线提供了强有力的工具。正确应用人工智能技术的特性，可以实现在漏洞挖掘、未知漏洞猎捕、漏洞优先级排序、漏洞修复等关键环节的自动化和精细化管理，从而显著提高安全漏洞的防御能力。这些技术的应用，不仅优化了安全防护流程，还加强了对潜在威胁的预见性和响应速度，为构建更加稳固的网络安全环境提供坚实基础。

01 **在漏洞挖掘方面，融合人工智能技术与程序分析，能够实现自动化安全漏洞挖掘。**传统的安全漏洞挖掘更多依赖于专家的深厚知识，且通常效率较为低下。相比之下，结合人工智能技术的漏洞挖掘方法在提升效率和降低成本方面表现突出。由 ForAllSecure 开发、并获得美国国防高级研究计划局（DARPA）资助的智能化漏洞挖掘系统 Mayhem，已在美军中得到广泛应用，显著提升了安全防护的效率和自动化水平。

02 **在未知漏洞猎捕方面，基于相似度算法和 AI Agent 模式 0day 漏洞归因定性，能够实现自动化 0day 猎捕。**人工智能技术结合 HTTP 文本向量化技术，存储通用攻击向量和历史攻击向量。首先通过弱信号发现疑似 0day 漏洞攻击向量，其次再结合向量相似度算法比对攻击流量向量与历史攻击向量，筛除已知漏洞攻击，再结合 AI Agent 模式 0day 归因定性，完成漏洞属性的填充，实现自动化 0day 猎捕。深信服自研的安全 GPT 检测大模型，致力于针对 0day 等高对抗攻击，实现全覆盖、零绕过，可以实现实时抓取流量、实时检测，深度挖掘传统安全设备难以检测的高对抗、高绕过的 Web 攻击。自 2023 年 5 月发布至今，深信服安全 GPT 已经成功捕获了 300+ 个在野 0day 漏洞。

03 **在漏洞优先级排序（VPT）方面，人工智能结合 SSVC 决策树模型，能够快速推理决策出需要优先处置的漏洞。**人工智能技术结合安全知识图谱，可以实现从多源异构的公网情报、客户现网攻击流量以及漏洞影响资产中，分析提炼出漏洞相关的实体关系，并沉淀到知识图谱中，作为漏洞优先级排序的关键决策因子，使漏洞排序具备可解释性。深信服的检测大模型，在训练过程吸收了大量的安全知识和专家经验，不仅对于流量本身有深刻的理解，对细微特征关联也有很强的敏感性，可以实现高效的威胁检出，同时基于生成式大模型强大的生成能力，还能生成详细的分析结果，包括威胁摘要、攻击载荷提取、攻击意图和手法分析、修复建议等内容。

04 **在漏洞修复方面，借助人工智能技术化被动为主动，实现对潜在漏洞的预测和快速修复。**传统的漏洞修复方法需要较多的人工介入，过程繁琐且耗时，而融合 AIGC 技术的模糊测试自动生成触发代码并验证漏洞修复的效果，能够减少人工验证的时间和成本，提高修复的效率和准确性。深信服依托自研安全 GPT 已经建立了完善的漏洞管理机制，在 AI 大模型技术赋能下实现高效的漏洞识别、自动化的漏洞响应和全面的安全运营服务，可以快速响应和处理各类安全威胁，有效提升安全漏洞防护能力。

安全漏洞发展趋势总结与应对措施

安全漏洞发展趋势总结

为有效应对日益加快的漏洞发现和利用速度，必须采用更加智能化的漏洞防护策略。AI 技术的应用已经极大地加速了漏洞的利用过程，许多 0day 漏洞在公开披露的当天就可能遭到大规模的恶意利用。攻击者能够迅速开发出漏洞利用工具，在漏洞未修复的时间窗口内，发起广泛的攻击行动，从而拉开攻击与漏洞修复的时间差，不仅能取得更好的攻击效果，而且挖掘和利用成本更低。

随着 AI 技术在安全领域的应用逐步成熟，2024 年观察数据显示，最快在漏洞披露 22 分钟后就出现利用，这使得防御者几乎没有时间来部署修复措施。面对这种严峻的形势，传统的安全防护措施在 AI 驱动的网络攻击面前显得力不从心。因此，迫切需要将 AI 技术融入到漏洞防护中，建立起智能化的安全防御体系，在与 AI 驱动的威胁对抗中取得先机。

近一年来，第三方组件、移动设备的漏洞利用上升趋势明显，需重点关注。第三方组件 0day 漏洞利用越来越多，攻击者更倾向于通过这些组件发起供应链攻击，利用其中的漏洞来渗透目标系统。针对移动设备的 0day 漏洞利用手段升级，近一半被用于执行间谍活动，进一步凸显了移动安全的重要性。

漏洞修复不彻底导致新的 0day 漏洞频繁出现，需要重点加强漏洞根因修复。近年来，通过对已修复漏洞的绕过或者修复不彻底漏洞的变体利用形成新的 0day 漏洞现象在近几年屡次出现。主要由于漏洞根本问题没有得到解决，使得攻击者能够通过不同的路径重新触发原始漏洞。所以 0day 漏洞的发现和修复，都仍存在很大的提升空间。为了有效应对这一挑战，需要产品提供者加强对漏洞更新的深入分析，不仅仅关注当前漏洞表现，更需要通过根本原因分析来修复漏洞，并加强修复后的测试工作，确保补丁有效率。这不仅能够减少新漏洞的产生，还能够提高整体的安全防护水平，构建更为稳固的安全防线。

开源软件漏洞治理措施建议

01

一是支撑政府加快制定开源软件漏洞风险防范相关的政策制度，推动开源软件漏洞监管工作落地执行。结合各地行业数字化转型安全保障要求，制定适用于当地重点行业领域的开源软件漏洞治理规范要求；监管单位内部及各关键基础设施机构所使用的开源代码安全，保障数字政府建设的安全可靠；配套出台漏洞激励机制，吸引社会白帽群体积极参与开源漏洞的发现与修复工作。

02

二是推动软件供应链上下游构建开源漏洞协同治理体系。开源软件安全漏洞的治理应贯穿开源软件设计、开发、发布、下载、运行等全生命周期各个阶段，相关参与主体应树立开源漏洞安全责任意识，尽最大可能保障开源软件的安全开发、安全托管、安全分发和安全运行。**开发者方面，**鼓励开发者树立安全开发意识，具备安全开发能力，在代码提交、合并前进行充分的安全测试。**代码托管平台方面，**对平台所托管的开源项目提供代码安全管理环境和漏洞风险监控服务，对于长时间未得到漏洞修复的开源项目，应控制其传播范围。**开源组织方面，**开源基金会、开源社区等对开源项目开展安全风险监控，统筹协调漏洞上报、验证、修复等工作，包括且不限于提供必要的技术支持和资源工具、建设开源项目漏洞安全评估管理体系、周期性对开源项目群进行安全评估等。对于安全漏洞治理周期长且安全风险高的开源项目，考虑实行退出机制。**开源软件使用者方面，**如软件开发商、系统集成商面向市场或消费者提供软件产品、服务，应作为第一责任人应承担整个软件产品、服务的漏洞测试、修复等工作，应关注软件产品中开源软件的漏洞通报和更新提醒，对受影响用户进行安全风险提示，及时组织力量进行漏洞修复和补丁发布，替换长时间未进行漏洞修复的组件，控制软件产品安全漏洞的影响范围。

03

三是鼓励高校、科研院所与社区联合开展开源漏洞治理人才培育与评价工作。打造开源安全人才培养路径与人才认证体系，构建产教融合机制，共享安全技术、工具和平台等教培资源，加强人才战略储备，积极营造“开放、合作、创新、共享”文化氛围。

04

四是重视科研创新，加强开源漏洞系列标准、工具的研制与应用推广。科研院所、高校、企业联合开展开源安全技术攻关，研制开源软件安全开发测试、漏洞挖掘与检测、漏洞分析与验证、软件供应链漏洞风险评估等标准和工具，鼓励利用人工智能大模型新兴技术开展相应领域技术攻关，并在国内代码托管平台 Gitee、Gitlink、Atomgit 等开展应用推广。

攻防场景下安全漏洞治理措施建议

从防御视角来看，0day 高可利用漏洞的检测和防护能力将成为保障网络安全的关键。通过对近年来攻防场景中 0day 高可利用漏洞进行分析，发现 0day 高可利用漏洞主要呈现以下特点：一是 0day 高可利用漏洞主要以获取系统权限为主；二是商业办公系统应用广泛、暴露面大、漏洞易被利用，导致其 0day 漏洞利用频率最高；三是 0day 漏洞利用更具有隐蔽性。因此，对于企业而言，提升 0day 高可利用漏洞的检测和防护能力至关重要，是保障企业网络安全的关键。从防御的角度来看，不同的 0day 漏洞影响不同的攻击面，这就要求用户在漏洞攻击的各个环节保护其远程服务，对权限、身份等控制面进行有效的监控和管理。面对海量漏洞风险告警，防守者需要更加关注攻击成功事件，建设攻击成功的研判能力和闭环处置流程。

01

从防御视角来看，及时发现并修复通用组件 Nday 漏洞是保障网络安全的基础工作之一。通过对近年来攻防场景中利用的 Nday 漏洞进行分析，发现利用频率较高的 Nday 漏洞，主要集中在使用范围较广泛的组件上，如 docker、Nacos、Oracle WebLogic 和 JBOSS 等组件。随着 Nday 漏洞的工具化、集成化，Nday 漏洞早已成为攻击通用目标的首选，因漏洞未及时修复而被攻陷的事件时常发生。因此，对 Nday 的防护显得尤为重要，因为它直接关系到整个防御体系的稳固性。防护 Nday 漏洞不仅是攻防场景中的一个重要环节，更是保障网络安全的基础工作之一。通过加强对 Nday 漏洞的管理和防护，可以有效提升系统的安全性，减少被攻击的风险。

02

从防御视角来看，错综复杂的漏洞利用路径要求企业采取全方位的安全防护措施，包括供应链、边界及内网的安全防护。在攻防场景下，攻击者越来越倾向于利用供应链中的漏洞进行攻击，这种攻击方式不仅可以扩大攻击范围，还具备较强的隐蔽性；随着边界安全对抗升级，通过加密、混淆等方式改造攻击流量，可以绕过安全设备的防护策略，突破边界安全防线；在横向阶段，利用 0day 漏洞、1day 漏洞等攻击手段获取集权设备的权限，进而控制整个内网。错综复杂的漏洞利用路径给企业安全防护带来了严峻挑战，这要求企业采取全方位的安全防护措施，包括供应链、网络边界和内网的安全防护，以提升企业整体的安全防护能力。

03

人工智能场景下安全漏洞治理措施建议

人工智能技术极大提升了安全漏洞防护水平

在漏洞检测与挖掘方面，人工智能技术与程序分析相结合，实现了自动化的安全漏洞挖掘，显著提升了 0day 漏洞的发现能力；漏洞优先级排序方面，人工智能能够快速分析并确定漏洞的严重程度，帮助组织有效分配资源，优先解决最关键的问题；漏洞修复方面，人工智能技术让漏洞修复变得更加高效和主动。

人工智能自身带来的安全漏洞隐患仍需重点关注，尤其是大模型核心生产模块的上下游交互过程

大模型安全包括应用安全、数据安全、系统安全和人员安全，涉及安全漏洞的风险问题主要分布于模型平台安全、供应链安全、信息和内容安全。其中大模型的核心生产服务模块在自身与外部交互的输入输出环节存在的安全风险最多，频繁出现敏感信息泄露、输入输出安全验证、访问控制和权限管控等问题。

生成式人工智能在安全漏洞的检测和防御领域逐渐渗透，众多网络安全公司引入生成式人工智能技术，在推出应对漏洞检测与防御的安全大模型上竞相发力

谷歌推出了经过安全用例训练的大语言模型 Sec-PaLM，融合了 Google 安全情报能力，包括 VirusTotal 和 Mandiant 等对漏洞、恶意软件和威胁行为者的情报。SentinelOne 的人工智能驱动行为分析引擎能够检测零日漏洞和未知威胁，提供攻击防护、恶意进程终止及损害修复功能。Zscaler 的 LLM 集成于全球最大的安全云中，利用处理超过 3900 亿笔交易和阻止 900 万个威胁的数据湖，有效识别并阻止未经授权的访问。深信服自研的安全大模型，基于多年安全数据进行预训练与微调，利用自研的 AI 安全大脑，可以实现精准识别高级威胁、自动化安全值守。

附录 参考链接

https://www.cnnvd.org.cn/home/loophole

https://nvd.nist.gov/vuln

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

https://github.com/cisagov/vulnrichment

https://www.bitsight.com/resources/slicing-through-cisas-kev-catalog

https://www.reversinglabs.com/blog/cisas-new-vulnrichment-program-attempts-to-address-nvd-slowdown

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends

https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

https://github.blog/news-insights/research/the-state-of-open-source-and-ai/#take-this-with-youautolink

https://talk.gitee.com/report/china-open-source-2023-annual-report.pdf

https://github.com/ossf

https://mp.weixin.qq.com/s/LohWtX1qdRRNIVZ_pBuZjg

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cyber-security-rules-for-digital-products-and-ancillary-services_en

https://www.cisa.gov/resources-tools/resources/2023-2025-strategic-plan

http://netinfo-security.org/CN/10.3969/j.issn.1671-1122.2022.03.005

报告编写工作组

工业和信息化部电子第五研究所软件与系统研究院

工业和信息化部电子第五研究所（中国赛宝实验室）（以下简称“电子五所”），始建于 1955 年，是工业和信息化部的直属事业单位，中国最早从事可靠性与环境适应性研究的权威机构。电子五所作为国家网络安全智库单位、国家信息安全漏洞库一级技术支撑单位、开放原子开源基金会开源漏洞信息共享项目主席单位，对外提供软件产品可信评估、开源软件安全合规检测、网络安全攻防综合服务、大模型测试服务、数据安全与个人信息安全评估服务等系列服务。重视网络安全人才队伍建设，成立赛宝月牙湖战队，开展网络空间安全对抗技术的前沿研究与创新应用，支撑国家级网络安全攻防任务。

关注【中国赛宝实验室】官方微信订阅号，

了解更多行业资讯、法规标准、组织动态、培训 / 活动信息。

深信服千里目安全技术中心

深信服千里目安全技术中心专注网络安全各技术领域研究及应用，囊括六大技术实验室和一个创新研究院，专注国内外漏洞、攻防对抗、终端安全、威胁情报、AI 等前沿技术的研究及应用，并最终赋能于产品。

关注【深信服千里目安全技术中心】微信公众号，第一时间了解更多安全漏洞情报和技术动态。

工业和信息化部电子第五研究所
（中国赛宝实验室）
CEPREI

SANGFOR
深信服科技

中国赛宝实验室
官方公众号

中国赛宝实验室
官方小程序

深信服官方微信

深信服移动官网