天融信 TOPSEC
002212.SZ

可信网络 安全世界

2024年

网络空间安全漏洞态势分析研究报告

天融信科技集团

2025年1月

目录

第一章 前言

在信息时代，数据安全和隐私保护已成为全球关注的焦点。随着技术进步和数字化进程的加速，安全漏洞问题愈发凸显，对各行各业构成了严峻挑战。2024 年，安全漏洞的发展呈现出新的特点和趋势。零日漏洞的利用持续增长，尤其是黑客组织和网络犯罪团伙越来越多地利用这些漏洞以实现对攻击目标的长期控制。新兴技术领域，如云计算、物联网、车联网、人工智能等，成为安全漏洞的重点领域。随着大模型技术的不断发展也会针对性的出现一些攻击手法，例如模型文件植入恶意代码、LLMjacking、数据投毒攻击、推理攻击、模型越狱攻击等等。2024 年的网络安全形势依旧严峻，重大失泄密事件接连发生，涉及多个国家，波及电信、医疗、云服务等多个关键行业，暴露出相关领域的诸多安全漏洞。这些事件不仅给国家、企业和个人带来了巨大影响，也促使全球加强国家安全、数据安全和个人隐私保护，共同应对挑战。

年初，某 VPN 被曝出存在零日漏洞，导致全球数千台设备被入侵，受害者包括政府和军事部门、金融机构以及技术公司等。 此外，某公司高管的电子邮件账户遭到攻击，黑客通过入侵获取了大量敏感信息，影响范围广泛。 医疗行业也未能幸免。2 月，美国最大的医疗处方服务商遭受勒索软件攻击，导致美国医疗保健系统中断数周，许多药店和医院无法处理药品订单和接收付款。 攻击者利用泄露的凭据闯入系统，窃取了包括姓名、社会保险号、诊断信息、治疗方案和财务数据等敏感信息，影响了数以百万计的个人。 7 月，知名网络安全公司 EDR 产品因一次错误的更新，导致全球数百万台计算机出现故障，严重影响了航空公司、银行、医院和政府服务的正常运行。此次事件暴露了数字基础设施的脆弱性，引发了公众对网络安全监管的广泛讨论。

作为中国领先的网络安全、大数据与云服务提供商，天融信始终以捍卫国家网络空间安全为己任，创新超越，致力于成为民族安全产业的领导者、领先安全技术的创造者和数字时代安全的赋能者。为了更好地了解网络空间安全漏洞的发展趋势，并采取适当的措施应对漏洞威胁，特发布《2024 年网络空间安全漏洞态势分析研究报告》。本报告旨在全面梳理和分析 2024 年网络空间安全漏洞的态势和特点并结合实例剖析典型安全事件的成因和影响以期为政府、企业和个人提供有针对性的防护建议和措施建议共同应对网络安全挑战维护网络空间的安全与稳定。

本报告重点内容共分两个部分，第一部分为 2024 年漏洞趋势，通过对国家漏洞库及前 100 个在野利用漏洞进行综合分析而产生。据 CNVD 公开数据显示，2023 年共披露漏洞 18635 个，2024 年共披露漏洞 18782 个，同比增加 0.79%。这可能表明新的攻击面被发现。其中，低危漏洞占 4.20%，中危漏洞占 48.86%，高危漏洞占 46.94%。相对于低危漏洞，中危和高危漏洞的数量要多得多，这也需要安全运维人员提高警惕，加强对中高危漏洞的控制。

第二部分为天融信 2024 年度高危漏洞预警情况概述，在 2024 年整个年度中，天融信阿尔法实验室监测发现了上万条漏洞情报，经过情报人员快速研判分析，第一时间预警并处理了多起突发高危漏洞，并根据漏洞的影响范围、影响对象及产生威胁的因素，挑出了排名前十的漏洞。2024 年度重点漏洞含 Windows 远程桌面许可服务远程代码执行漏洞、Apache Tomcat 远程代码执行漏洞、Microsoft Outlook 远程代码执行漏洞、Palo Alto Networks PAN-OS 存在命令注入漏洞等。天融信第一时间监测到漏洞后，进行了漏洞复现和应急响应处理，并给出临时解决方案，保障了客户网络空间安全。

企业安全部门应该提升网络安全威胁感知能力，建立有效的监测预警体系，并制定应急指挥计划，加强对威胁的发现、监测、预警和应对能力。以便在网络攻击发生时快速作出应对。此外，还需要强化攻击溯源能力，重点建设辅助攻击溯源相关能力（如授权控制、流量记录），使得对网络攻击的溯源工作更加轻松，以便有效地防御和应对来自外部的网络攻击。

第二章 国家漏洞库概况

天融信阿尔法实验室秉承攻防一体的理念，以保卫国家网络空间安全为己任，在未来的工作中将持续针对网络空间漏洞进行实时侦测，并灵活应对和防护突发漏洞的产生，攻防相结合，为国家及客户安全进行全方位赋能。

漏洞的统计与评判是评估网络安全情况的一个重要指标，天融信阿尔法实验室参考国家漏洞数据库数据，对 2024 年披露的漏洞进行了全方位的统计分析，下图是近十年漏洞数量走势图，从这个数据中可以看出，近十年来，CNVD 披露的漏洞数量总体呈现上升趋势。尤其是在 2018 年至 2021 年之间，漏洞数量大幅增加。2024 年来看，漏洞数量出现了上升，这种变化可能是网络安全生态系统中各种因素交互作用的结果，可能是由于新的安全技术的采用，使得更多的漏洞被发现和披露，也可能是由于黑客行为的调整，他们可能更专注于利用那些尚未被修复的漏洞。同时，随着软件系统复杂性的增加和互联设备的激增，新的漏洞也在不断产生。与此同时，我们也不能忽视网络安全仍然面临着多样化和不断变化的威胁，因此需要保持高度警惕，不断创新和完善网络安全防护措施。

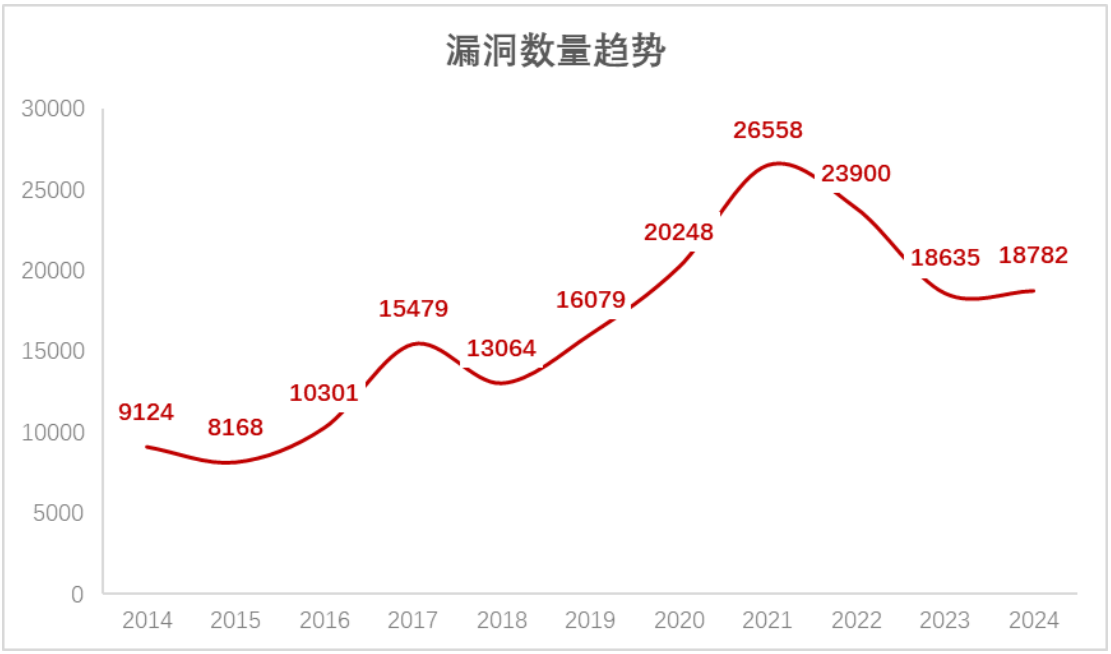


图 1 近十年漏洞数量走势图(数据来自于 CNVD)

漏洞威胁等级统计

根据 2024 年 1-12 月漏洞引发威胁严重程度统计，其中低危漏洞占 4.20%，中危漏洞占 48.86%，高危漏洞占 46.94%。

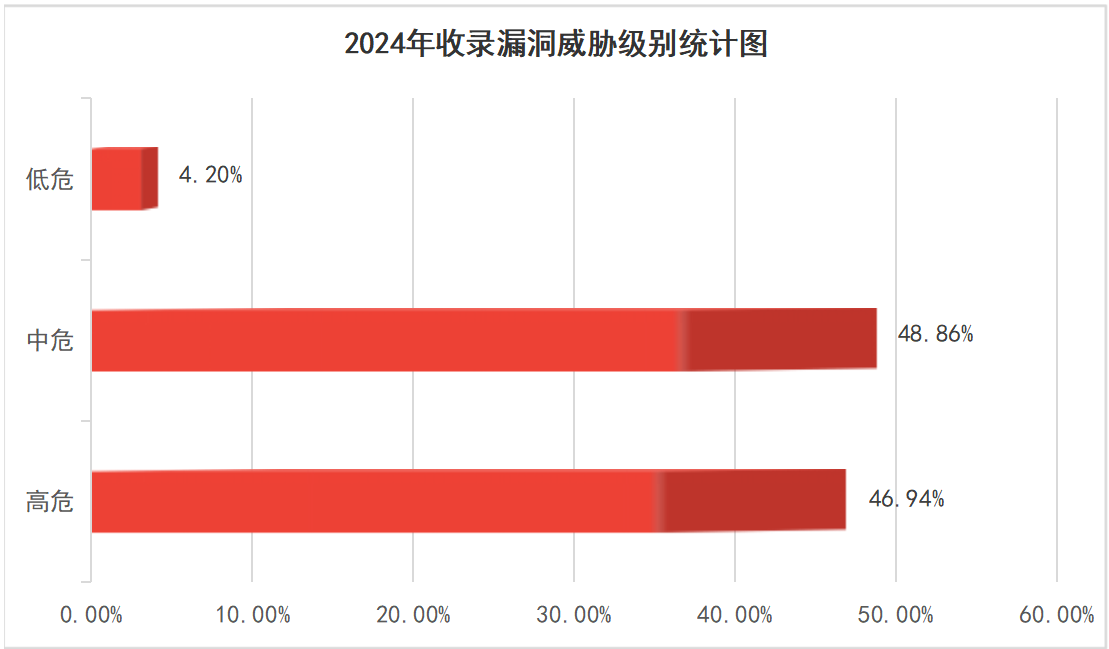


图 2 2024 年收录漏洞按威胁级别统计(数据来自于 CNVD)

分析 2023 年到 2024 年漏洞威胁统计的变化，低危漏洞的比例从上年的 5.85%降到了 4.20%，这背后反映出安全团队在处理基础性问题上变得更加敏锐和高效。中危漏洞的比例则从 46.93%攀升至 48.86%，这一增长不容忽视，意味着面对的中等风险问题比以前更多了，需要投入更多的精力去解决。至于高危漏洞，虽然比例小降至 46.94%，但这个数字依然很高，也从侧面证明了在关键安全领域所做的努力开始见到成效。

漏洞影响对象类型统计

根据 2024 年 1-12 月漏洞引发威胁统计，受影响的对象大致可分为九类：分别是 WEB 应用、应用程序、网络设备、智能设备、操作系统、工业控制系统、安全产品、数据库、车联网系统。其中 WEB 应用漏洞 48.10%，应用程序漏洞 24.50%，网络设备漏洞 13.80%，智能设备漏洞 5.00%，操作系统漏洞 4.00%，工业控制系统漏洞 1.90%，安全产品漏洞 1.30%，数据库系统漏洞 1.30%，车联网系统漏洞 0.10%。

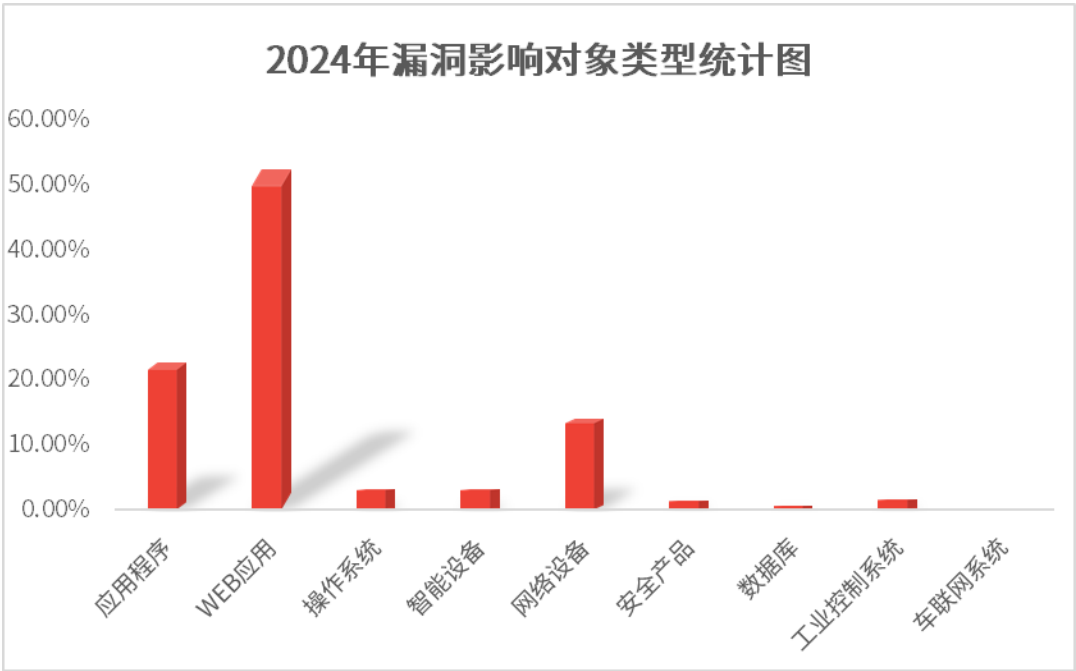


图 3 2024 年漏洞影响对象类型统计(数据来自于 CNVD)

2024 年的漏洞统计数据中表明，WEB 应用仍然是最受攻击者青睐的目标，占据了近一

半的漏洞比例。应用程序紧随其后，显示出软件开发过程中仍然存在不少安全隐患。网络设备虽然稍有下降，但依然占据了 13.80%的比例，表明这些基础设施的安全性不容忽视。

值得注意的是，智能设备的漏洞比例上升到了 5.00%，这反映了随着物联网技术的普及，相关设备的安全问题日益突出。操作系统和工业控制系统的漏洞分别占到了 4.00%和 1.90%，尽管比例不高，但由于它们在关键业务中的核心地位，任何安全漏洞都可能带来严重的后果。安全产品本身也未能幸免，1.30%的漏洞比例提醒我们，即便是用于保护系统的工具也需要不断审视和加固。数据库系统的漏洞同样占到了 1.30%，强调了数据存储和管理环节的重要性。车联网系统虽然仅占 0.10%，但在汽车智能化的趋势下，这一领域的安全挑战不容小觑。

数字化持续地赋能汽车产业，汽车已经从传统的出行工具逐渐演变成了新一代的移动数据中心和互联网服务创新的重要平台，智能网联汽车已成为汽车产业转型升级、交通方式变革、智慧城市建设的重要方向。未来，天融信将持续深耕车联网安全领域，全力构建智能网联汽车产业安全生态体系，为建设交通强国贡献企业力量。

漏洞产生原因统计

根据 2024 年 1-12 月漏洞产生原因的统计，设计错误导致的漏洞占比 67.70% ，屈居首位，紧跟其后的是输入验证错误导致的漏洞占比 26.20%，位居第二，接着是边界条件错误导致的漏洞占比 3.50%，位居第三。后面的其他错误、访问验证错误、竞争条件配置错误分别占比 1.60%、 0.90%、0.10%、0.01%。

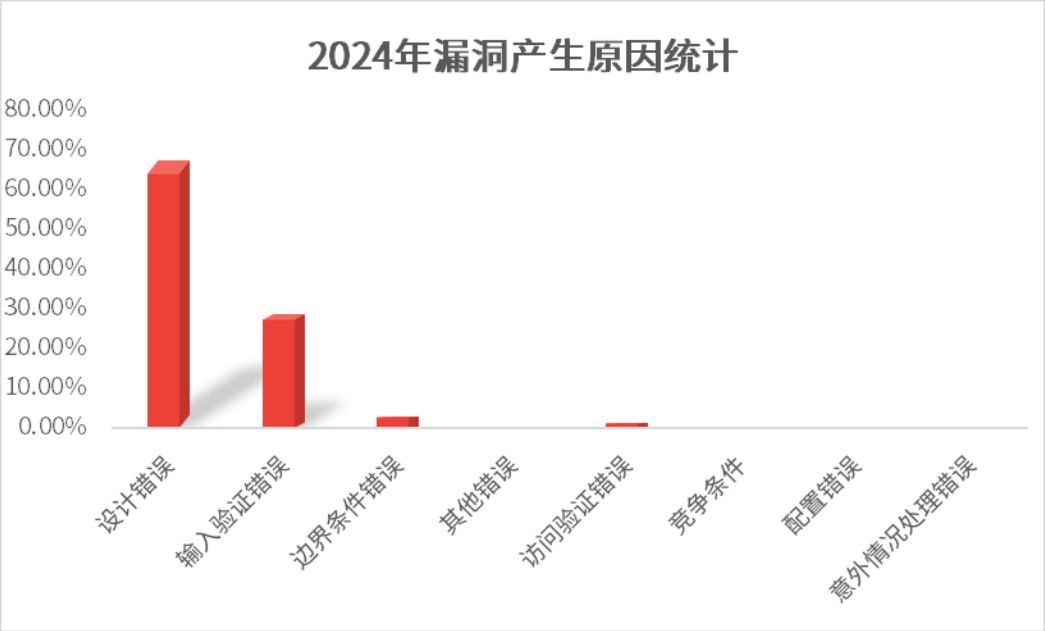


图 4 2024 年漏洞产生原因统计（数据来自于 CNVD）

漏洞的产生原因统计表明，设计错误仍然是安全漏洞的主要来源，占据了绝大部分的比例。这反映出在软件和系统的初期设计阶段，安全考量仍然存在不足。紧随其后的是输入验证问题，这类错误表明开发者在处理用户输入时仍需更加严谨，以防止潜在的安全威胁。边界条件处理不当也是一大隐患，说明系统在应对极端或非预期情况时的健壮性有待提升。此外，其他类型的错误，如访问验证、竞争条件配置等问题，虽然占比相对较小，但也提醒我们在开发过程中不能忽视任何细节。

漏洞引发威胁统计

根据 2024 年 1-12 月漏洞引发威胁统计，未授权的信息泄露占比 53.70%位居首位，管理员访问权限获取占比 27.50%位居第二，拒绝服务占比 8.30%位居第三，后面的未授权的信息修改、普通用户访问权限获取、其它。占比分别是 8.30%、0.10%、0.01%。

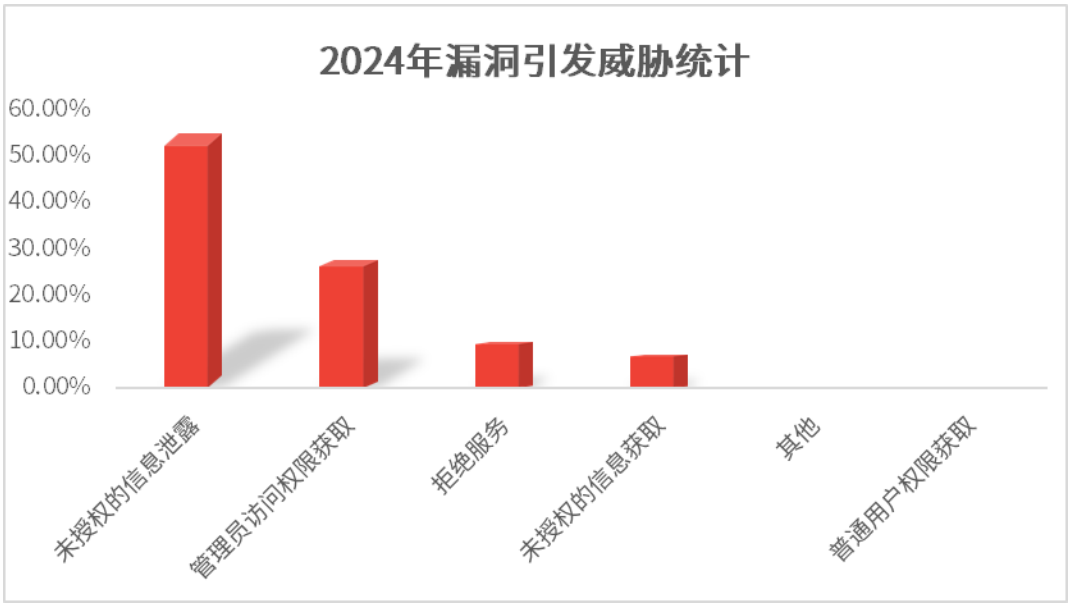


图 5 2024 年漏洞引发威胁统计（数据来自于 CNVD）

在漏洞引发的威胁统计中，未授权的信息泄露依然是最突出的安全挑战，占据了最大的比例。这可能与数据的广泛使用和存储方式有关，反映出数据保护仍然是网络安全的重中之重。获取管理员访问权限的威胁紧随其后，显示出攻击者对高权限目标的持续兴趣。拒绝服务和未授权的信息修改虽然占比相对较低，但仍然可能对业务运营造成显著影响，需要引起足够的关注。相比之下，普通用户访问权限获取和其他类型的威胁影响较小，但仍需在全面的安全策略中加以考虑。

在数据流转监测方面，天融信数据安全风险分析系统可以通过监控分析绘制全景图，并根据预设规则与算法，快速识别异常，持续分析数据流向，洞察潜在威胁，实现敏感数据监测和溯源，确保企业数据的安全合规使用。而天融信 API 安全审计系统则可以通过 API 审计、访问控制与权限审核、API 传输内容智能识别、数据流转监控与防护及溯源机制等模块，助力企业掌握自身数据资产分布以及数据流向路径监测，及时发现和处置潜在的数据安全风险。

行业漏洞收录统计

根据 2024 年 1-12 月行业漏洞统计，2024 年一共收录了电信行业漏洞 1677 个，移动互联网行业漏洞 990 个。工控行业漏洞 402 个。

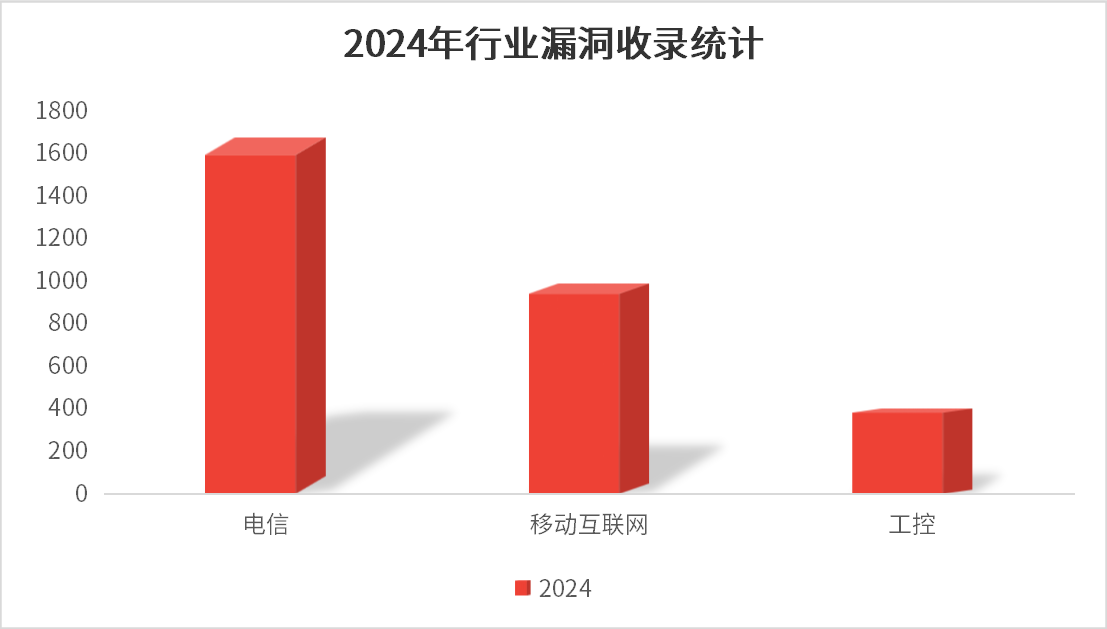


图 6 2024 年行业漏洞收录统计（数据来自 CNVD）

统计显示，电信行业和移动互联网行业的安全挑战尤为突出。电信行业的复杂技术和庞大用户基础使其成为网络安全的重点关注对象，需要不断优化安全策略以保护通信网络和用户数据。移动互联网行业则因数字化转型加速，应用和服务激增，带来了更多的安全风险，企业必须加强安全开发和应急响应能力。

相比之下，工控行业的漏洞数量较少，但这一领域的安全问题不容忽视。工业控制系统通常用于关键基础设施，如电力、水利和交通等。随着工业互联网的发展，这些系统与外界的连接增加，面临的网络威胁也在上升。尽管当前工控系统的封闭性提供了一定的安全保障，但关键基础设施的安全不容忽视，行业应提前布局，强化网络安全防护。

漏洞修复情况统计

根据 2024 年 1-12 月漏洞修复情况统计，漏洞数量排名前列的厂商与其修复数量如下图，其中 Apple、Oracle、IBM、Cisco、PDF-XChange、Dell 漏洞修复率均为 100%，其余厂商中 Linux、Adobe、Intel、Google、Microsoft、WordPress、SAMSUNG、友讯、腾达、Campcodes、吉翁电子，漏洞修复率分别为 99.88%、99.80%、99.33%、99.23%、98.75%、89.94%、88.98%、75.72%、71.91%、50.00%、49.02%。

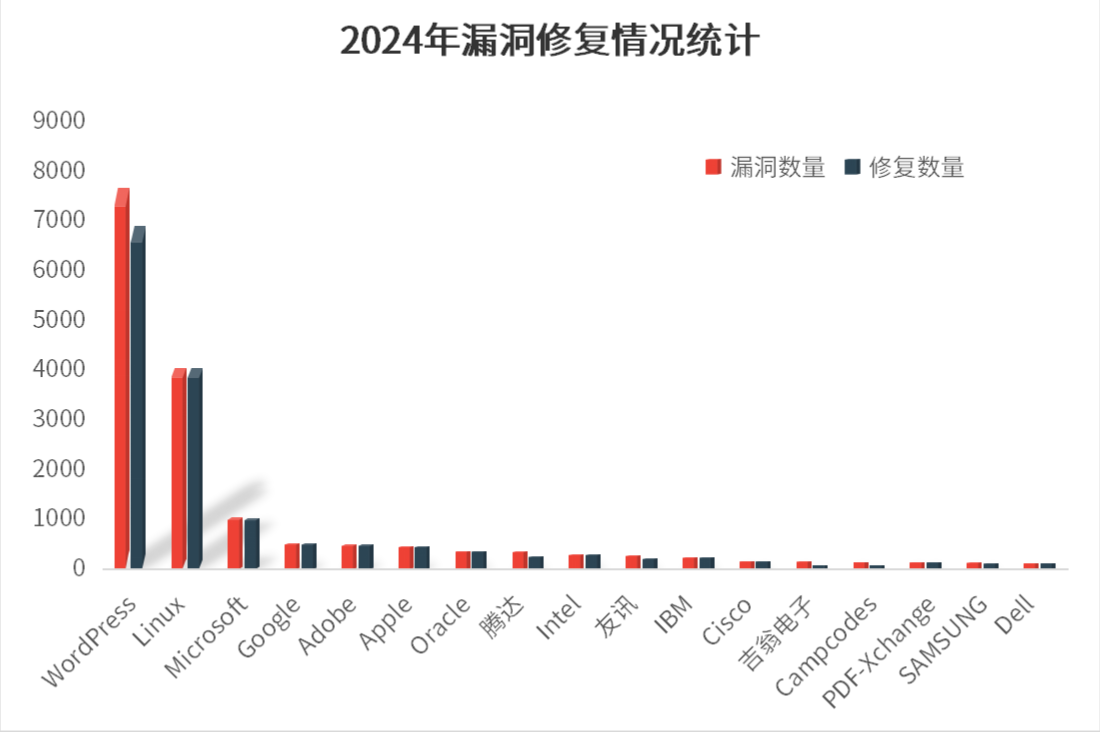


图 7 2024 年漏洞修复情况统计（数据来自 CNNVD）

数据显示，Apple、Oracle、IBM 和 Cisco 等科技巨头成功实现了所有已知漏洞的修复，彰显了它们对网络安全的高度重视。Dell 同样表现优异，确保了其产品和服务的安全性。其他厂商如 Linux、Adobe、Intel 和 Google 等也展示了较高的修复效率，尽管未达到 100%，但仍迅速应对并修补了大部分安全问题。Microsoft 和 WordPress 等平台在面对较大用户基数和技术复杂度的情况下，也取得了不错的修复成绩。

然而，部分厂商如 SAMSUNG、友讯和腾达等在漏洞修复方面遇到了更多挑战，修复率相对较低，表明它们可能需要进一步加强安全流程和技术能力。

漏洞增长趋势

通过 CNVD 漏洞信息库对 2023、2024 漏洞公开数据显示，2023 年一共披露漏洞 18635 个，2024 年一共披露漏洞 18782 个。同比 2023 年增加 0.79%，2023 年高危漏洞 8800 个，2024 年高危漏洞 8819 个，同比 2023 年增加 0.22%，2023 年中危漏洞 8745 个，2024 年中危漏洞 9174 个，同比 2023 年增加 4.91%，2023 年低危漏洞 1090 个，2024 年低危漏洞 789 个，同比 2023 年减少 27.61%。

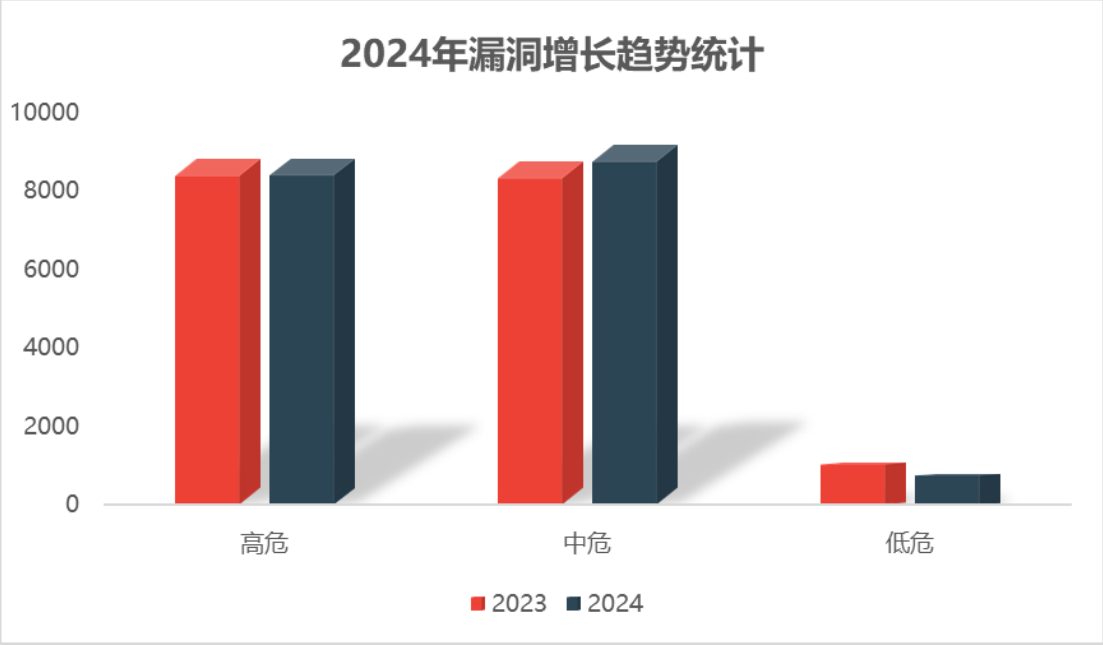


图 8 2024 年漏洞增长趋势统计（数据来自 CNVD）

2024 年的漏洞披露情况与前一年相比略有变化。总体来看，2024 年公开的漏洞数量基本保持稳定，仅小幅增长。高危漏洞的数量略有增加，显示出安全社区在应对严重威胁方面

还需要加强。中危漏洞也有所增加，表明这一类别的漏洞仍然受到广泛关注和重视。与此同时，低危漏洞的数量显著下降，这可能反映了厂商和研究人员更加聚焦于解决那些对系统安全影响较大的问题。

整体趋势显示，尽管新发现的漏洞总数没有大幅波动，但不同类型漏洞的变化反映出安全领域内的优先级调整和技术进步。高危和中危漏洞的增加提醒我们，仍需持续关注并加强这些潜在风险点的防护。低危漏洞的减少则可能意味着资源更多地被分配到了更紧迫的安全问题上，体现了安全策略的优化。

第三章 在野利用漏洞概况

通过对全网漏洞数据的分析统计,我们筛选了 2024 的前 100 个在野利用漏洞进行统计分析。此次统计分析主要从漏洞所影响厂商、影响平台产品、漏洞类型以及 EXP 公开情况等 4 个方面展开。结果显示，漏洞影响厂商前三名分别是 Microsoft、Palo Alto Networks、Fortinet。从影响的平台产品进行统计，受影响的平台大致可分为五类:分别是操作系统、软件平台、路由器和交换机等、远程管理托管面板以及 CRM 系统。其中操作系统 19%，占据首位。由此可见漏洞依然集中在主流操作系统中。

在前 100 个在野利用漏洞中大约有 72.00%存在公开 EXP，这一数据令人担忧，意味着一旦这些漏洞被曝光，攻击者几乎可以立即获得现成的工具来发动攻击。这不仅缩短了从发现到利用的时间窗口，也使得企业面临的网络安全风险急剧上升。

从漏洞类型来看，OS 命令注入、身份验证绕过、代码注入是当前网络安全形势下最为严峻的威胁。由于许多漏洞可能是由于人为错误而引起的，因此提高员工的安全意识和教育是非常重要的。包括定期进行安全培训，提供安全指南，以及定期进行安全检查和测试。具体统计分析结果如下:

漏洞影响厂商分布情况

根据 2024 在野利用漏洞前 100 例所影响的厂商情况进行统计，前三名分别是 Microsoft、Palo Alto Networks、Fortinet。其中 Microsoft 的产品占比达到 11.00%，Palo Alto Networks 和 Fortinet 的产品均占到 6.00%。

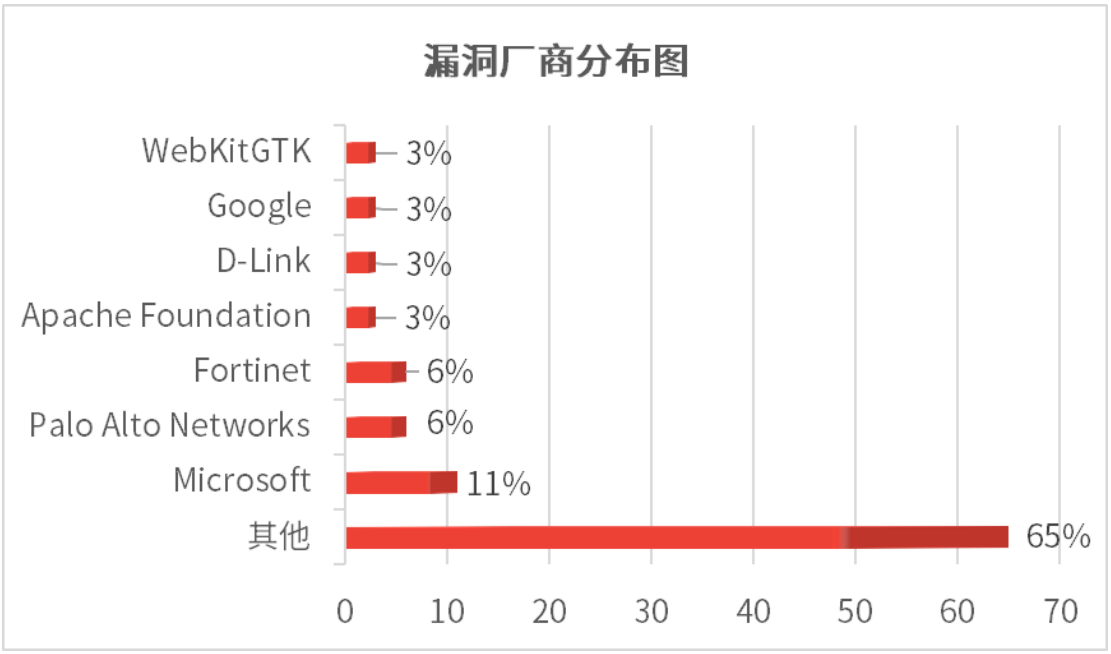


图 9 漏洞厂商分布图(数据来自于 cybersecurity-help)

2024 年，在野利用漏洞的影响主要集中在几家大型科技公司。Microsoft 依然是最受影响的厂商之一，其广泛使用的产品继续吸引着攻击者的注意。Palo Alto Networks 和 Fortinet 也进入了前三名，显示出网络安全设备和解决方案成为攻击者的新目标。这表明，即便是在安全领域领先的公司，也需要不断强化防护措施，以应对日益复杂的威胁。同时，用户和企业应及时更新补丁，确保系统安全。

漏洞影响平台产品分类

根据 2024 在野利用漏洞前 100 例所影响的平台产品情况进行统计，受影响的平台产品大致可分为五类：分别是操作系统、软件平台、路由器和交换机等、远程管理托管面板以及 CRM 系统。其中操作系统 19.00%、软件平台 12.00%、路由器和交换机等 6.00%、远程管理托管面板 4.00%、CRM 系统 4.00%、其他平台 55.00%。

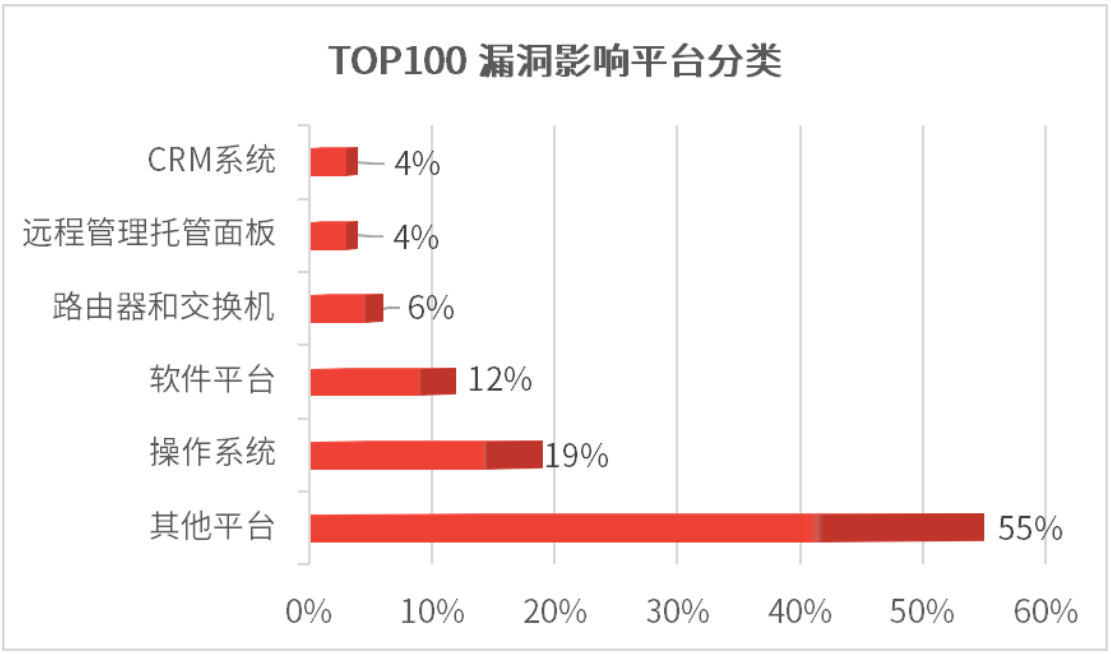


图 10 TOP100 漏洞平台分类(数据来自于 cybersecurity-help)

2024 年数据显示，操作系统仍然是最受攻击者青睐的目标之一，尽管其比例有所变化。软件平台紧随其后，成为另一个重要的受攻击领域，这可能与越来越多的企业依赖复杂的软件生态系统有关。路由器和交换机等网络设备也受到了一定关注，反映出这些基础设施组件的安全性至关重要。远程管理托管面板和 CRM 系统同样未能幸免，表明企业内部管理和客户关系管理系统的安全防护同样不容忽视。

值得注意的是，还有相当一部分漏洞影响了其他类型的平台，这凸显了网络安全威胁的多样性和广泛性。整体来看，这些数据反映了攻击者对不同平台的兴趣分布，同时也提醒企业和用户在选择和使用各类技术产品时，必须高度重视安全问题，及时更新补丁，加强防护措施。

漏洞类型统计概况

根据 2024 在野利用漏洞前 100 例漏洞类型情况进行统计，其中 OS 命令注入（CWE-78）占比最多，以 14.00%位居首位，身份验证绕过（CWE-287）占比 10.00%，代码注入（CWE-94）

占比 7.00%，路径遍历（CWE-22）占比 6.00%，访问控制（CWE-284）占比 6.00%，输入验证不当（CWE-20）占比 5.00%，释放后重引用（CWE-416）占比 4.00%，缓冲区溢出（CWE-119）占比 4.00%，其他类型占比 44%。

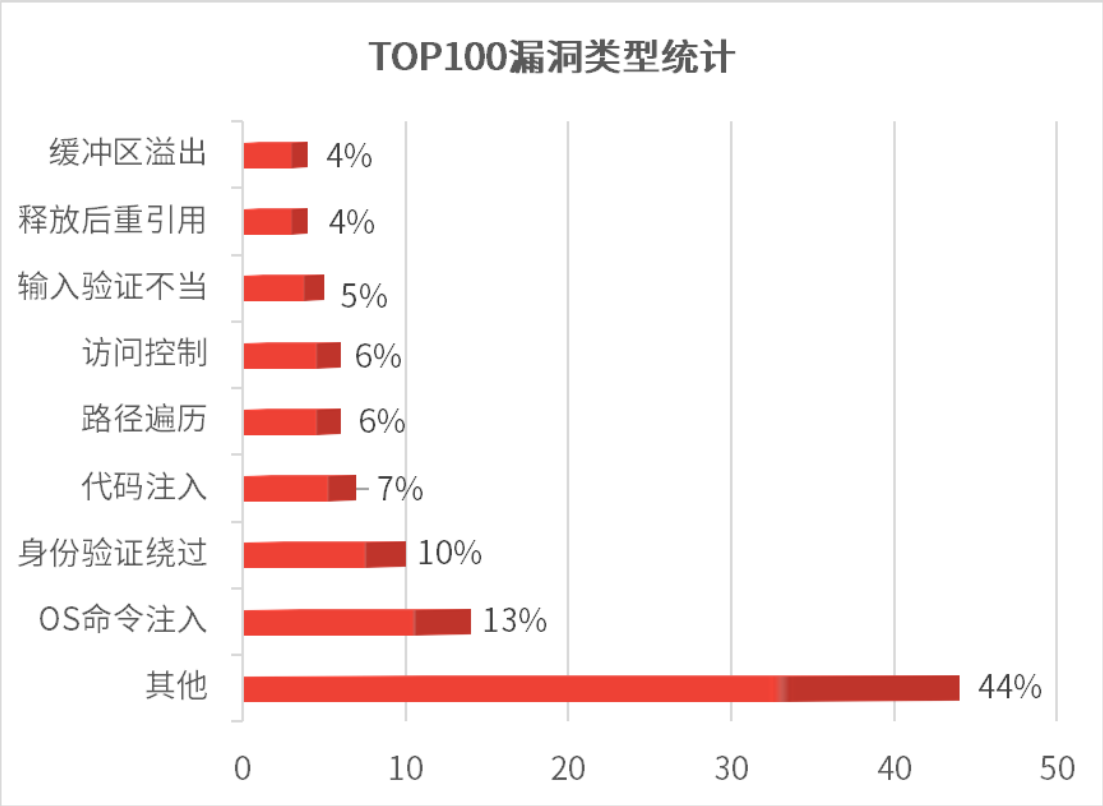


图 11 TOP100 漏洞类型统计概况(数据来自于 cybersecurity-help)

根据 2024 年在野利用漏洞的统计分析，OS 命令注入成为最常见的攻击手段，反映出攻击者倾向于通过操作系统层面的漏洞来实施攻击。身份验证绕过问题也十分突出，表明攻击者持续寻找突破安全屏障的方法。代码注入和路径遍历等传统漏洞类型依然常见，提醒开发者需重视安全编码实践。访问控制和输入验证不当的问题同样值得关注，强调了企业在应用程序开发中加强安全措施的重要性。此外，释放后重引用和缓冲区溢出等较为特殊的漏洞类型也时有发生，提示开发者需全面考虑各种潜在的安全风险。总体而言，这些趋势揭示了当前网络安全的重点领域，企业应加强对操作系统的防护，同时关注软件平台的身份验证机制和输入处理逻辑。

根据 MITRE 今年通过对公开可用的国家漏洞数据库中 31770 项数据调研分析得出的 CWE TOP 25 排名如下。

排名	ID	名称	KEV 占比	与 2023 年排名相比
1	CWE-79	跨站脚本	3	1
2	CWE-787	越界写入	18	-1
3	CWE-89	SQL 注入	4	0
4	CWE-352	跨站请求伪造（CSRF）	0	5
5	CWE-22	路径遍历	4	3
6	CWE-125	越界读取	3	1
7	CWE-78	OS 命令注入	5	-2
8	CWE-416	Use-After-Free	5	-4
9	CWE-862	缺少授权	0	2
10	CWE-434	危险文件上传	0	0
11	CWE-94	代码注入	7	12
12	CWE-20	输入验证不当	1	-6
13	CWE-77	命令注入	4	3
14	CWE-287	身份验证不当	4	-1
15	CWE-269	权限管理不当	0	7
16	CWE-502	反序列化	5	-1
17	CWE-200	信息泄露	0	13
18	CWE-863	授权错误	2	6
19	CWE-918	服务器端请求伪造（SSRF）	2	0

20	CWE-119	缓冲区溢出	2	-3
21	CWE-476	NULL 指针解引用	0	-9
22	CWE-798	硬编码凭证	2	-4
23	CWE-190	整数溢出	3	-9
24	CWE-400	不受控制的资源消耗	0	13
25	CWE-306	缺少关键功能的身份验证	5	-5

表 1 CVE TOP 25 排名(数据来自于 MITRE)

与过去几年一样，CWE 团队在分析今年的变化时指出，前 25 名的漏洞越来越多地转向内存安全、权限管理和访问控制，在今年的漏洞排行榜上，有几种漏洞类型的排名与去年有所变化，其中有的完全消失或是首次进入前 25 名。

排名大幅提升的漏洞有：

（1） CWE-352（CSRF）：从第 9 名提升到第 4 名；

（2） CWE-94（代码注入）：从第 23 名提升到第 11 名；

（3） CWE-269（权限管理不当）：从第 22 名提升到第 15 名；

（4） CWE-863（授权错误）：从第 24 名提升到第 18 名；

排名大幅下降的漏洞有：

（1） CWE-20（输入验证不当）：从第 6 名下降到第 12 名；

（2） CWE-476（NULL 指针解引用）：从第 12 名下降到第 21 名；

（3） CWE-190（整数溢出）：从第 14 名下降到第 23 名；

（4） CWE-306（缺少关键功能的身份验证）：从第 20 名下降到第 25 名；

Top 25 中的新入围的漏洞有：

（1） CWE-400（不受控制的资源消耗）：从第 37 名上升到第 24 名；

（2） CWE-200（信息泄露）：从第 30 名上升到第 17 名；

从 Top 25 中落选的漏洞有：

（1） CWE-362（竞争条件）：从第 21 名降至第 34 名；

（2） CWE-276（权限不当）：从第 25 名降至第 36 名；

EXP 公开情况统计

根据 2024 在野利用漏洞前 100 例 EXP 公开情况进行统计，其中公开 EXP 稍多，占比 72.00%，未公开 EXP 的为 28.00%。

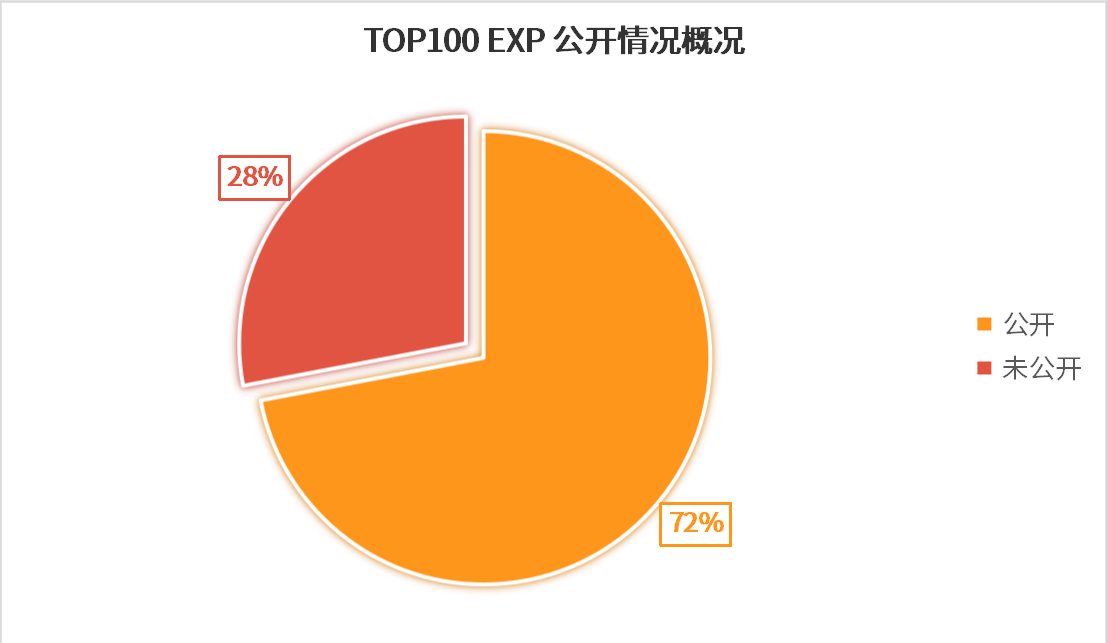


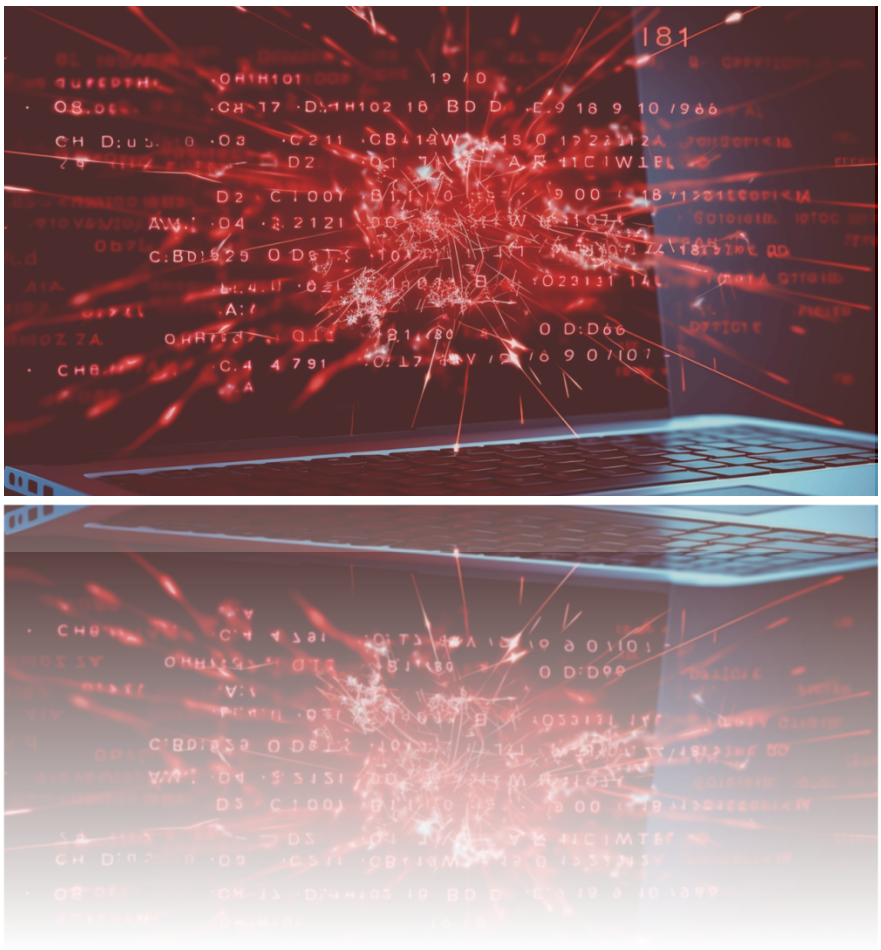
图 12 TOP100 EXP 公开情况概况(数据来自于 cybersecurity-help)

2024 年，在野利用漏洞的情况发生了显著变化，尤其是在漏洞利用工具（EXP）的公

开程度上。随着安全社区和研究人员对漏洞披露的关注增加，越来越多的漏洞在发现后不久便伴随有详细的攻击方法和工具。这一趋势使得安全团队能够更快地研究和修复问题，但同时也为潜在的攻击者提供了现成的攻击手段，加速了从理论风险到实际威胁的转化。

对于企业来说，这种变化意味着需要更加警觉。不仅要关注官方的安全公告，还要留意地下论坛和其他渠道中的最新威胁情报。为了应对快速变化的威胁环境，企业应建立敏捷的安全响应机制，确保能迅速识别并修补可能被利用的漏洞。

值得注意的是，即使是一些未公开 EXP 的漏洞，也构成了不小的风险。由于缺乏具体的攻击细节，这些漏洞更难防范。因此，企业除了传统的补丁管理和配置加固外，还应该加强内部的安全测试和审计，主动寻找并修复潜在的安全隐患。与专业的安全服务提供商合作，借助他们的经验和资源，也是提升整体安全水平的重要途径。



第四章 漏洞预警统计情况

2024 年，天融信阿尔法实验室通过漏洞监测系统共监测发现各类漏洞信息 38429 条，经过漏洞监测系统自动智能筛选后留存高危漏洞信息 317 条，经过人工专家进一步研判后，最终发布了 52 条高危漏洞风险提示通告。涉及众多厂商的软件产品，由漏洞引发的安全威胁也多种多样，统计结果显示，主流操作系统是漏洞高发产品。2024 年针对 Microsoft 厂商漏洞预警次数达 16 次，其中 Windows 系统的漏洞占大多数。

2024 年预警的漏洞中，远程代码执行漏洞在漏洞类别中的显著占比，达到 40%。这一类漏洞一直都是 APT 攻击者的重要方向和攻击武器，攻击者利用这类漏洞可以远程执行任意代码或者指令，有些漏洞甚至无需用户交互，这使得他们能够在未被察觉的情况下渗透目标系统并潜伏其中。对目标网络和信息系统造成严重影响。具体预警统计分析情况如下:

漏洞厂商情况

在 2024 年内发布的 52 条漏洞通告内所涉及到的知名厂商中，针对 Microsoft 厂商漏洞预警次数最多，为 16 次，占比约 31%，Apache 和 Atlassian 都是 4 次，占比 8%，并列第二名。

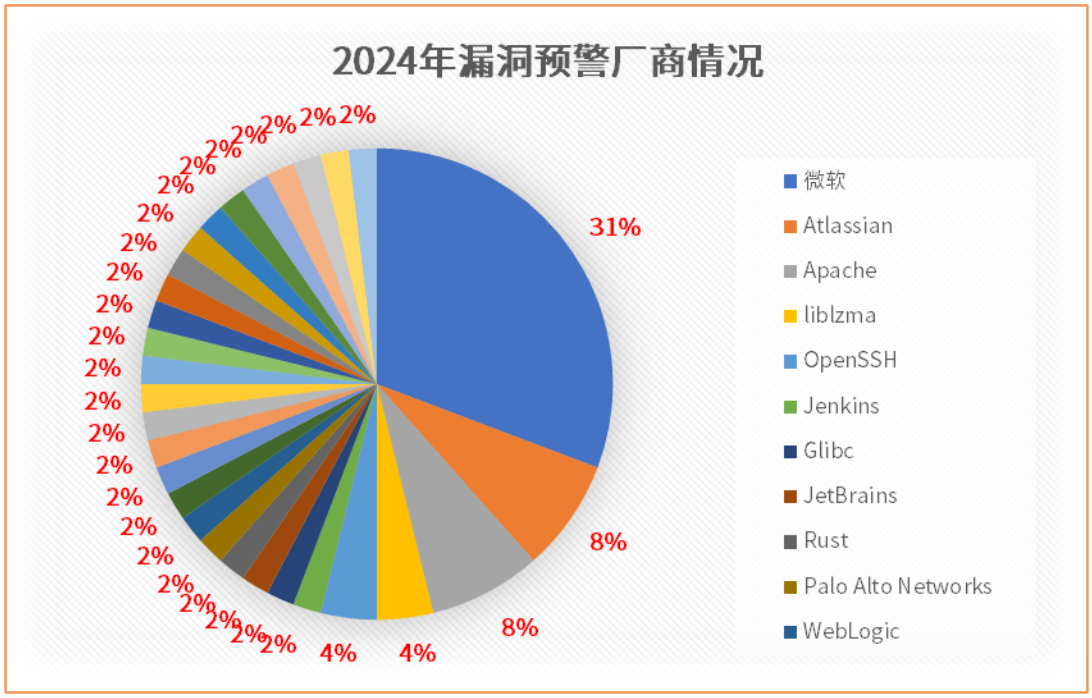


图 13 2024 年漏洞预警厂商情况

从漏洞预警情况来看，微软预警数量最多，主要由于其高市场占有率、广泛使用和产品复杂性。作为全球最受欢迎的操作系统和办公软件供应商，Windows、Office、Exchange 等产品广泛应用于个人、企业和政府机构，吸引了攻击者的关注。微软产品功能复杂且生态庞大，为兼容新旧系统往往增加安全管理的难度。同时，其披露透明度较高和漏洞赏金计划吸引了大量研究者进行漏洞挖掘。尽管漏洞数量较多，微软通常能够及时发布补丁，用户只需保持更新即可降低风险。这些因素表明，微软漏洞数量多更多是其产品普及度和透明度的结果，而非安全性差的表现。

从预警分布数据来看，微软、Apache、Atlassian 等广泛使用的平台和工具均存在安全问题，这主要源于代码质量、复杂性和安全设计等因素。微软系列因其用户基数庞大、功能复杂以及历史遗留代码问题，成为漏洞多发的重点对象。而像 Apache、OpenSSH 等开源软件，由于代码公开，虽然便于社区审查，但也容易被攻击者利用。商业软件如 Atlassian、GitHub 和 Sonatype Nexus Repository，因其处理企业敏感数据而成为攻击目标。网络安全设备和服务软件（如 Palo Alto Networks 和 WebLogic）通常处于企业核心网络中，

其漏洞对安全影响尤为严重。此外，特定行业软件由于场景定制化，可能在安全设计上考虑不足。这些系统在企业和政府机构中得到了广泛应用，涉及大量敏感信息和数据，如客户资料和财务信息等。一旦这些软件遭受攻击或数据泄露，可能会给企业和用户带来重大损失。

减少漏洞的关键在于严格代码审查、强化安全设计、改进开发流程，并结合漏洞响应机制，快速修复和更新，降低风险与影响。

漏洞威胁情况

在 2024 年发布的 52 条漏洞通告中，所通告的漏洞可分为 10 大类，分别是远程代码执行漏洞、身份验证绕过漏洞、SQL 注入漏洞、任意文件上传漏洞、命令注入漏洞、路径遍历漏洞、供应链投毒漏洞、文件读取漏洞、堆溢出漏洞、权限绕过漏洞，其中远程代码执行漏洞占比 40%，位于首位，身份验证绕过漏洞占比 12%，并列位于第二位。

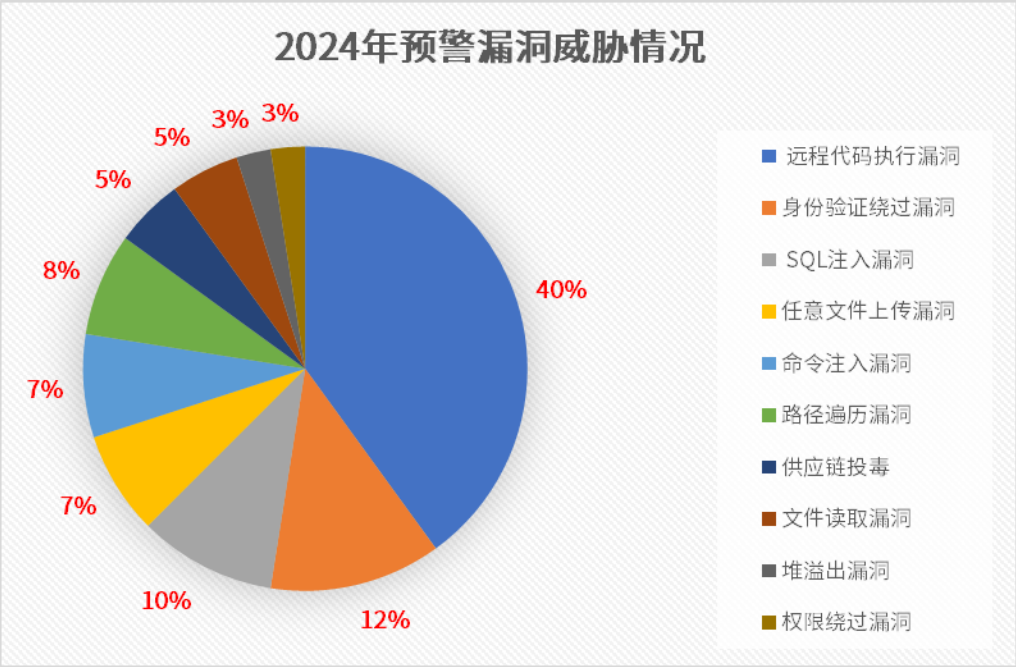


图 14 2024 年预警漏洞威胁情况

由此可见，远程代码执行漏洞依然备受攻击者的青睐，因为远程代码执行漏洞一旦被攻击者利用，攻击者可以通过它完全控制目标系统、窃取和篡改数据、扩大攻击范围，导致严

重的安全事故。其次是身份验证绕过漏洞、SQL 注入漏洞和任意文件上传漏洞的占比较高。通过身份验证绕过漏洞的预警详情来看，由于程序对身份验证不完全或者身份验证存在逻辑错误，导致攻击者绕过正常的验证流程，通过未授权直接上传 webshell 等利用方式，实现对目标系统的完全控制。部分身份验证绕过漏洞可能会造成个人隐私信息、用户金融信息、企业商业机密等敏感信息泄露。SQL 注入漏洞可能获取数据库中的敏感信息，如用户凭证，系统信息被恶意篡改或者删除。文件上传漏洞可以让攻击者上传恶意脚本或者 WebShell，使其获得服务器的权限。在其他漏洞类型中，虽然命令注入漏洞、文件读取漏洞等的出现频率和占比相对较小，但它们所带来的危害往往不可忽视，甚至可能具有更大的破坏性，必须给予足够的重视。

企业在面对漏洞时，应保持积极的安全态度，采取综合性措施来防范和修复漏洞。通过定期漏洞扫描、加强输入验证、实施最小权限原则、及时打补丁、建立日志监控机制，并进行安全审计和代码审查，可以有效降低漏洞的风险。同时，企业应考虑漏洞的潜在影响，尽快响应并修复发现的漏洞，确保系统的安全和稳定运行。

年度 TOP10 高危漏洞

本节内容筛选自天融信 2024 年预警的漏洞信息，并根据漏洞的利用难易程度、漏洞利用成功后造成的损失、漏洞影响的范围进行排名，根据排名节选出排名前十的漏洞。

危害程度排名	漏洞编号	标题	概述
NO.1	CVE-2024-38077	Windows 远程桌面许可服务远程代码执行漏	远程桌面许可服务（Remote Desktop Licensing，RDL）是 Windows Server 的一个组件，用于管理和颁发远程桌面服务的许可证，确保对远程应用程序和桌面进

		洞	行安全且合规的访问。RDL 服务不是默认安装，但很多管理员会手动开启。 此漏洞是 Windows Server RDL 服务中的一个堆溢出漏洞（CWE-122），由于在解码用户输入的许可密钥包时，未正确检验解码后数据长度与缓冲区大小之间的关系，导致堆溢出。此漏洞影响 Windows Server 2000 到 Windows Server 2025 所有版本，已存在近 30 年。未经授权的远程攻击者通过向存在漏洞的 Windows Server 发送特制的数据包来利用此漏洞，成功利用此漏洞可在该目标服务器上执行任意代码。
NO.2	CVE-2024-50379	Apache Tomcat 远程代码执行漏洞	该漏洞源于在不区分大小写的系统（如 Windows）与 Tomcat 在路径大小写敏感性处理上的不一致。当默认 Servlet 的 readonly 参数被设置为 false（非默认配置）并允许使用 PUT 方法上传文件时，攻击者能够上传包含恶意 JSP 代码的文件并通过条件竞争不断发送请求，触发 Tomcat 对其解析和执行，最终实现远程代码执行。
NO.3	CVE-2024-21413	Microsoft Outlook 远	未经身份验证的远程攻击者可以向受害者发送一封邮件，其中包含一个精心构造的

		程代码执行漏洞	恶意链接，然后诱骗受害者打开此链接。攻击者可以通过此漏洞绕过 Microsoft Office 的受保护的视图，使受害者通过此链接以 SMB 协议访问远程的资源，这会使用受害者的本地凭据进行 SMB 协议的身份认证，从而将受害者系统的本地 NTLM 哈希凭据泄露给攻击者。
NO.4	CVE-2024-3400	Palo Alto Networks PAN-OS 存在命令注入漏洞	Palo Alto Networks PAN-OS 软件的 GlobalProtect 功能中针对特定 PAN-OS 版本和不同功能配置的命令注入漏洞可能使未经身份验证的攻击者能够在防火墙上以管理员权限执行任意代码。
NO.5	CVE-2024-24576	Rust 命令注入漏洞	Rust 标准库命令注入漏洞（CVE-2024-24576，被称为 BatBadBut）在使用 API 在 Windows 上调用批处理文件（带有 bat 和 cmd 扩展名）时没有正确转义参数 Command。能够控制传递给生成进程的参数的攻击者可以通过绕过转义来执行任意 shell 命令。
NO.6	CVE-2024-36401	Geoserver 远程代码执行	GeoServer 调用的 GeoTools 库 API 会以不安全的方式将要素类型的属性名称传递给 commons-jxpath 库，该库在评估 XPath 表达式时可以执行任意代码。多个 OGC 请求参数允许未经身份验证的用户

			通过针对默认 GeoServer 安装的特制输入进行远程代码执行 (RCE)。
NO.7	CVE-2024-40629	JumpServer 任意文件写入漏洞	攻击者可以利用 Ansible playbook 写入任意文件，从而导致 Celery 容器中出现远程代码执行 (RCE)。Celery 容器以 root 身份运行并具有数据库访问权限，这允许攻击者窃取主机的所有机密、创建具有管理员权限的新 JumpServer 帐户或以其他方式操纵数据库。
NO.8	CVE-2024-21683	Atlassian Confluence 远程代码执行漏洞	经过身份认证的远程攻击者通过构造特殊的请求，利用该漏洞在受影响的机器上执行任意代码。
NO.9	CVE-2024-21007	WebLogic T3 IIOP 远程代码执行漏洞	未经身份验证的攻击者通过 T3、IIOP 进行网络访问来破坏 Oracle WebLogic Server,利用该漏洞在远程服务器上执行任意代码，从而获取到远程服务器的权限。
NO.10	CVE-2024-27348	Apache HugeGraph-Server Gremlin 远程命令执行漏洞	由于 1.0.0 到 1.3.0 版本默认未开启身份验证，攻击者可通过直接访问 RESTful API 执行 Gremlin 命令，查询其中数据。利用该漏洞可以在受影响的机器上执行任意代码。

表 2 TOP10 危害排名

漏洞预警 TOP10 漏洞回顾

一、Windows 远程桌面许可服务远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2024-38077

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

漏洞评分：9.8

预警日期：2024-08-09

漏洞描述：CVE-2024-38077 被命名为“狂躁许可（MadLicense）”。远程桌面许可服务（Remote Desktop Licensing，RDL）是 Windows Server 的一个组件，用于管理和颁发远程桌面服务的许可证，确保对远程应用程序和桌面进行安全且合规的访问。该服务被广泛部署于开启了 Windows 远程桌面服务（3389 端口）的服务器上。RDL 服务不是默认安装，但很多管理员会手动开启。

此漏洞是 Windows Server RDL 服务中的一个堆溢出漏洞（CWE-122），由于在解码用户输入的许可密钥包时，未正确检验解码后数据长度与缓冲区大小之间的关系，导致堆溢出。未经授权的远程攻击者通过向存在漏洞的 Windows Server 发送特制的数据包来利用此漏洞，成功利用此漏洞可在该目标服务器上执行任意代码。

二、Apache Tomcat 远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2024-50379

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

漏洞评分：9.8

预警日期：2024-12-18

漏洞描述：该漏洞源于在不区分大小写的系统（如 Windows）与 Tomcat 在路径大小写敏感性处理上的不一致。当默认 Servlet 的 readonly 参数被设置为 false（非默认配置）并允许使用 PUT 方法上传文件时，攻击者能够上传包含恶意 JSP 代码的文件并通过条件竞争不断发送请求，触发 Tomcat 对其解析和执行，最终实现远程代码执行。

三、Microsoft Outlook 远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2024-21413

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

漏洞评分：9.8

预警日期：2024-02-23

漏洞描述：Outlook 是微软办公软件套装 Microsoft Office 的组件之一，Outlook 可以用来收发电子邮件、管理联系人信息、记日记、安排日程、分配任务。

未经身份验证的远程攻击者可以向受害者发送一封邮件，其中包含一个精心构造的恶意链接，然后诱骗受害者打开此链接。攻击者可以通过此漏洞绕过 Microsoft Office 的受保护的视图，使受害者通过此链接以 SMB 协议访问远程的资源，这会使用受害者的本地凭据进行 SMB 协议的身份认证，从而将受害者系统的本地 NTLM 哈希凭据泄露给攻击者。

成功利用此漏洞，会导致受害者的本地 NTLM 凭据泄露或在攻击者机器上实现远程代码执行。

四、Palo Alto Networks PAN-OS 存在命令注入漏洞

漏洞类型：命令注入

漏洞编号：CVE-2024-3400

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

漏洞评分：10.0

预警日期：2024-04-16

漏洞描述：PAN-OS 是 Palo Alto Networks 公司开发的下一代防火墙操作系统，。PAN-OS 提供了一整套高级安全功能，结合深度包检测和威胁防护，帮助企业保护其网络基础设施。

Palo Alto Networks PAN-OS 软件的 GlobalProtect 功能中针对特定 PAN-OS 版本和不同功能配置的命令注入漏洞可能使未经身份验证的攻击者能够在防火墙上以管理员权限执行任意代码。

五、Rust 命令注入漏洞

漏洞类型：命令注入

漏洞编号：CVE-2024-24576

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

漏洞评分：10.0

预警日期：2024-04-12

漏洞描述：Rust 标准库命令注入漏洞（CVE-2024-24576，被称为 BatBadBut）在使用 API 在 Windows 上调用批处理文件（带有 bat 和 cmd 扩展名）时没有正确转义参数 Command。能够控制传递给生成进程的参数的攻击者可以通过绕过转义来执行任意 shell 命令。

BatBadBut 是一个漏洞，允许攻击者 CreateProcess 在满足特定条件时对间接依赖该函数的 Windows 应用程序执行命令注入。BatBadBut 漏洞可能影响 Erlang、Go、Haskell、Java、Node.js、PHP、Python、Ruby、Rust 等多种编程语言。

六、Geoserver 远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2024-36401

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

漏洞评分：9.8

预警日期：2024-07-03

漏洞描述：CVE-2024-36401 是 GeoServer 中的一个高危远程代码执行漏洞。GeoServer 是一个用 Java 编写的开源服务器，允许用户共享和编辑地理空间数据。该漏洞源于 GeoServer 调用的 GeoTools 库 API 会以不安全的方式将要素类型的属性名称传递给 commons-jxpath 库，该库在评估 XPath 表达式时可以执行任意代码。多个 OGC 请求参数允许未经身份验证的用户通过针对默认 GeoServer 安装的特制输入进行远程代码执行（RCE）。

七、JumpServer 任意文件写入漏洞

漏洞类型：文件写入漏洞

漏洞编号：CVE-2024-40629

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

漏洞评分：9.8

预警日期：2024-07-19

漏洞描述：具有低权限用户帐户的攻击者可以利用 Ansible playbook 写入任意文件，从而导致 Celery 容器中出现远程代码执行 (RCE)。Celery 容器以 root 身份运行并具有数据库访问权限，这允许攻击者窃取主机的所有机密、创建具有管理员权限的新 JumpServer 帐户或以其他方式操纵数据库。

八、Atlassian Confluence 远程代码执行漏洞

漏洞类型：远程命令执行

漏洞编号：CVE-2024-21683

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

漏洞评分：8.8

预警日期：2024-05-30

漏洞描述：Atlassian Confluence 是由 Atlassian 开发的一款企业级协作软件，用于团队知识管理、文档协作和项目管理。Confluence 提供了一个统一的平台，团队成员可以轻松创建、共享和管理信息，提升工作效率和协作效果。

经过身份认证的远程攻击者通过构造特殊的请求，利用该漏洞在受影响的机器上执行任意代码。

九、WebLogic T3 IIOP 远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2024-21007

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

漏洞评分：7.5

预警日期：2024-04-18

漏洞描述：未经身份验证的攻击者通过 T3、IIOP 进行网络访问来破坏 Oracle WebLogic Server,利用该漏洞在远程服务器上执行任意代码，从而获取到远程服务器的权限。

十、Apache HugeGraph-Server Gremlin 远程命令执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2024-27348

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

漏洞评分：9.8

预警日期：2024-06-03

漏洞描述：Apache HugeGraph 是一个开源的图数据库系统项目，它提供了易用、高效和通用的图数据存储和分析解决方案。建议受影响用户尽快升级到安全版本。由于 1.0.0 到 1.3.0 版本默认未开启身份验证，攻击者可通过直接访问 RESTful API 执行 Gremlin 命令，查询其中数据。利用该漏洞可以在受影响的机器上执行任意代码。

第五章 总结

2024 年数据显示了网络安全领域的几个趋势：尽管公开披露的漏洞总数保持相对稳定，但高危漏洞的比例增加，表明严重性较高的漏洞更受攻击者青睐，对关键基础设施和企业系统构成更大威胁。中危漏洞数量的增长也值得注意，因为它们在特定情境下同样可能导致严重后果，而低危漏洞的减少可能反映了资源更多地投入到更严重的漏洞研究与修复上。这些变化强调了网络安全环境的复杂化，要求企业和组织不仅要快速响应高危漏洞，也要持续监控管理中低危漏洞，并通过建立完善的漏洞处理流程、加强合作信息共享、应用人工智能和自动化工具、强化内部安全培训等措施，构建多层次防御体系以应对不断演变的安全挑战。

通过对 2024 年前 100 个在野利用漏洞统计看出，Microsoft、Palo Alto Networks、Fortinet 为主要攻击目标，其余涵盖了操作系统、浏览器、固件、软件平台和服务器平台等多个领域。操作系统的漏洞依旧占据首位，28%的漏洞存在未公开 EXP，较往年有所降低。最严峻的威胁来自 OS 命令注入，身份验证绕过和代码注入等漏洞类型。应对措施需包括及时修复漏洞、强化访问控制、提升用户安全意识，并运用高级威胁防御技术，以确保综合网络安全。

2024 年的漏洞监测数据显示，尽管全年共监测到大量漏洞信息，但经过智能筛选和专家研判后，最终发布的高危漏洞风险提示相对较少，这表明漏洞监测系统的效率较高。微软作为最大的漏洞预警来源，其高发漏洞主要与其广泛的市场占有率和产品复杂性有关，但这并不一定意味着其产品安全性低下，而是反映了其较为透明的漏洞披露政策和庞大的用户基础吸引了更多的安全研究和攻击关注。远程代码执行漏洞依然是攻击者的主要目标，因其能够赋予攻击者对目标系统的完全控制权，进而造成严重安全威胁。此外，身份验证绕过、

SQL 注入和任意文件上传等漏洞类型也占据了较高比例，这些漏洞若被利用，可能导致敏感信息泄露或系统被完全控制。因此，企业应保持高度警惕，通过定期漏洞扫描、加强代码审查、及时修补漏洞等综合性措施，来降低安全风险，确保信息系统安全稳定运行。

安全防护建议

在归纳 2024 年网络空间安全态势的过程中，我们也针对态势发展的新形势，提出了一些防护建议。

1. 漏洞扫描和渗透测试：漏洞扫描和渗透测试是确保信息系统安全的重要手段。定期进行这些测试可以帮助企业及时发现并修复潜在的安全隐患，防止攻击者利用已知或未知的漏洞发起攻击。为此，可以使用自动化安全扫描工具对系统进行全面扫描，能够快速识别已知漏洞，并提供详细的修复建议，覆盖广泛的资产和技术栈，确保不会遗漏任何关键区域。为了确保漏洞得到彻底修复，建议邀请独立的第三方安全团队进行复查。这些团队通常具备丰富的经验和专业的技术，能够从不同的角度评估系统的安全性，发现自动化工具可能忽略的问题，并模拟真实的攻击场景，验证现有防御措施的有效性。此外，漏洞扫描和渗透测试不应是一次性的活动，而应成为持续的安全管理流程的一部分。通过建立定期的扫描计划和应急响应机制，企业可以在漏洞被利用之前及时采取行动，减少安全风险。

2. 部署网络安全设备：使用防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）等网络安全设备是构建多层次防御体系的基础，能够有效监控和阻止潜在的威胁。企业应配置防火墙规则，限制对服务器的访问，仅允许特定的 IP 地址或 IP 段进行连接，从而减少外部攻击的风险并提高内部网络的安全性。对于关键业务系统，建议采用更严格的访问控制策略，如基于角色的访问控制（RBAC），确保只有授权人员能够访问敏感资源。同时，部署 IDS 和 IPS 可以实时监控网络流量，检测并阻止异常行为。这些系统通过分析网络日志、流量模式和已知攻击特征，及时发现并响应潜在的威胁，

特别是针对高级持续性威胁（APT）和零日攻击，提供额外的防护层，增强整体安全性。此外，部署 SSL 证书以加密传输，保护服务器与客户端之间的通信，防止数据在传输过程中被窃取或篡改，并提升用户对网站和服务的信任度。对于涉及敏感信息的业务，建议使用更强的加密协议，如 TLS 1.3，确保最高级别的安全性。

3. 安全意识培训：员工是企业网络安全的第一道防线，因此提升他们的安全意识和技术水平至关重要。通过系统化的安全培训，企业可以减少人为错误导致的安全事件，确保全体员工都能参与到网络安全工作中来。具体措施包括：培训员工识别常见的社会工程攻击手段，如钓鱼邮件、电话诈骗和虚假网站，通过模拟攻击演练和案例分析，帮助员工了解如何应对这些威胁，并养成良好的安全习惯，例如提醒员工不要轻易点击不明链接或下载附件，遇到可疑情况应及时上报；教育员工创建和使用强密码，避免使用简单的密码组合或重复使用密码，建议使用密码管理器来生成和存储复杂的密码，确保每个账户都有独特的凭证，此外，定期更改密码并启用多因素认证（MFA），可以进一步增强账户的安全性；鼓励员工在发现任何可疑活动时立即报告，无论是内部还是外部的威胁，建立畅通的沟通渠道和快速响应机制，确保安全团队能够在第一时间介入处理。通过这些措施来提高员工的安全技能，培养责任感和警觉性，形成全员参与的安全文化。

数字经济的发展为网络安全提出了更大的挑战与机遇，网络安全服务变得更为全面和多样化。近年来，以服务方式交付行业防护能力，同时构建“多层级、多角色线上线下协同”的安全运营体系是未来服务化发展的重点。天融信坚持安全与行业应用深度融合，以总部云服务平台为基石，依托遍布全国的监测能力中心，通过云端专家与线下服务人员协同，持续为全行业客户提供“网络+数据”线上线下一站式安全服务。

2025 年漏洞态势展望

随着技术的不断进步，网络安全漏洞的态势也在不断变化，对于我国网络安全漏洞态势来说，在近期的中央经济工作会议中明确了 2025 年的重要任务，其中第二条便是“以科技创新引领新质生产力发展，建设现代化产业体系”。随着新质生产力的提出，网络安全产业“国产化、行业化、服务化、智能化”的四化发展正式步入“新质网安”时代。

2025 年，预计有两个关键趋势将深刻影响漏洞的发展和应对策略。首先，漏洞披露与应急响应机制趋于更加完善，企业和政府机构将更加重视这一领域的建设和优化。其次，零日漏洞的发展趋势呈现出数量上升、受影响供应商数量增加以及被利用时间缩短等特点。

第一个关键趋势是漏洞披露与应急响应机制的完善，企业和政府机构对漏洞披露与应急响应机制的重视程度将显著提高。建立健全的漏洞收集、分析、通报和处置流程，不仅有助于提高漏洞处置的效率和准确性，还能有效降低漏洞被利用的风险。为了实现这一目标，企业需要采取如下一系列措施：

第一项是漏洞收集与报告，企业应建立一个开放且透明的漏洞提交平台，鼓励内部员工和外部安全研究人员积极报告发现的漏洞。通过提供奖励机制，如漏洞赏金计划，可以激励更多人参与到漏洞发现的过程中。

第二项是漏洞分析与分类，收到漏洞报告后，企业需要迅速组织专业的安全团队进行分析，评估漏洞的严重性和潜在影响。根据漏洞的影响范围和紧急程度，对其进行分类，以便优先处理高风险漏洞。

第三项是漏洞通报与协调，一旦确认漏洞的存在，企业应及时向受影响的用户、合作伙伴和其他相关方通报情况。同时，加强与其他安全组织和机构的合作与信息共享，确保漏洞信息能够快速传播，避免漏洞被恶意利用。例

如，美国证券交易委员会（SEC）要求企业在发现重大网络安全事件后的四个工作日内提交报告，这为企业提供了明确的时间框架。

 # 第四项是漏洞修复与验证，企业应在最短时间内开发并发布漏洞补丁或更新，确保用户能够及时应用修复措施。此外，邀请独立的第三方安全团队进行复查，确保漏洞得到彻底修复，防止攻击者利用残留的安全隐患。

 # 最后一项则是持续监控与改进，漏洞披露与应急响应机制不应是一次性的活动，而应成为企业安全管理体系中的常态化流程。通过定期回顾和优化漏洞处理流程，企业可以不断提高自身的安全防护水平。

第二个关键趋势是零日漏洞的发展趋势及应对策略，零日漏洞的数量继续上升，受影响的供应商数量也有所增加，攻击者利用这些漏洞的时间窗口也在缩短。面对这一严峻形势，企业必须采取如下更加积极主动的应对策略。

 # 第一项是加强安全监测与预警，企业应部署先进的安全监测系统，利用人工智能和机器学习技术实时分析网络流量和系统行为，及时发现异常活动。通过自动化工具，企业可以在零日漏洞被利用之前识别出潜在威胁，从而提前采取防御措施。

 # 第二项是推进安全左移，为了应对越发隐蔽、多变的攻击手段，企业需要将安全防护能力“左移”到应用的开发阶段，推动安全战略从“传统基于边界防护的安全”向“面向应用现代化的内生安全”模式转变。通过在开发过程中引入安全测试和审查机制，企业可以减少自研代码本身的缺陷，同时防范通过软件供应链引入的漏洞。

第三项是加强应急响应能力，企业应建立完善的应急响应计划，确保在发生零日漏洞攻击时能够迅速做出反应。通过定期开展实战化的攻防演练，企业可以检验网络安全体系建设的科学性和有效性，发现工作中存在的问题，并针对演练中发现的问题和不足之处进行持续优化。

第四项是促进国际合作与信息共享，在全球化的背景下，网络安全问题已经超越了国界。各国政府和企业应加强合作，共同应对跨国界的网络安全威胁。通过建立国际间的合作机制，分享最新的威胁情报和技术成果，可以有效提升全球网络安全的整体水平。

作为国内领先的网络安全、大数据与云服务提供商，天融信始终以捍卫国家网络空间安全为己任，创新超越，持续为客户构建更加完善的网络安全防御能力，为数字经济的发展保驾护航。天融信一直致力于积极发挥自身在监测预警与应急服务优势，全面掌握漏洞动态。通过多维度数据采集分析，敏感信息及时预警，持续深入信息安全领域的监测与应急工作，能够及时监测到网络空间的漏洞动态，提供快速的监测与预警服务。及时发现漏洞，就可以更快地采取应对措施，防止安全风险的扩散。通过对网络流量的监测，能够发现异常的网络活动、异常的系统行为等。这些信息可以及时发送到相关部门，使其采取必要的应对措施。

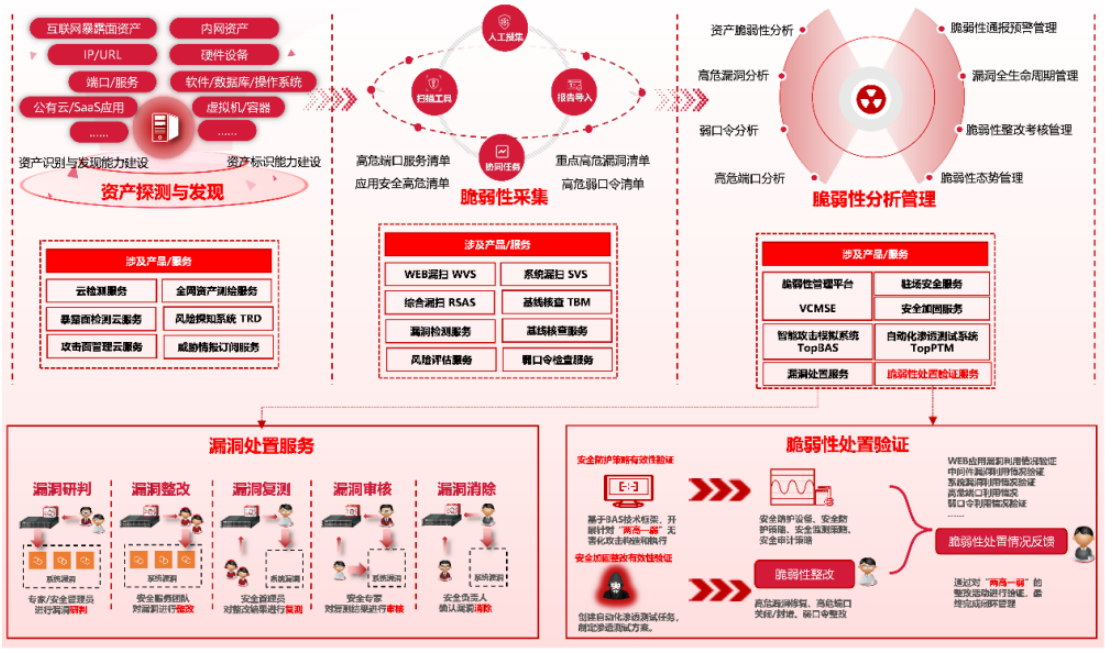
人工智能技术与各行业的战略融合，是牵引产业升级的原动力，孕育新质生产力的新引擎。在人工智能技术的加持下，算力、数据与模型有机融合，网络安全能力正不断被重塑，逐步进化为面向全能力的智能协同。天融信以大模型、小模型、机器学习等 AI 技术为核心，基于天问算力平台、训练平台、应用平台三大平台，构建企业级 AI 安全能力体系，实现 AI 全面赋能，在检测防护、安全运营、安全交付等多个场景中实现了提质增效。

漏洞防治解决方案

近年来，各行业主管部门对网络安全漏洞问题给予了高度重视，陆续发布《网络产品安全漏洞管理规定》、《网络产品安全漏洞收集平台备案管理办法（征求意见稿）》等政策文件，并持续开展诸如“两高一弱”、“数安护航”等专项整治行动，以加强网络安全管理。

天融信根据多年的信息安全领域研究成果和项目经验，推出资产探测与发现、脆弱性采集和脆弱性分析管理的“三步走”综合整治方案。该方案综合运用暴露面分析、资产探测识别、脆弱性评估等多项技术和产品，构建“检测、分析、处置、验证”全流程闭环的综合解决方案。

首先，对资产进行全量采集与发现，精准识别服务器、网络设备、数据库、主机等资产类型，建立资产台账、资产映射关系、网络拓扑图信息，为后续漏洞排查工作提供资产数据支撑。其次，基于 AI、UEBA 技术以及内外部权威漏洞库数据，采用“工具+人”相结合的方式开展对内外网系统和应用脆弱性检查与验证工作，确认漏洞的严重性和可利用性。最后，形成漏洞全生命周期管理闭环，持续跟踪脆弱性处置情况、资产状态、安全告警等数据，并向相关安全管理部门上报资产和脆弱性情况，根据实际情况对防范措施做进一步改进。



未来，天融信将充分发挥自身优势，坚持资产安全管理技术探索与实践，在保障客户网络安全的同时，努力践行领军企业的社会责任与担当，为国家网络安全整体能力建设做出贡献，为实施网络强国战略贡献企业力量。

天融信阿尔法实验室

天融信阿尔法实验室成立于 2011 年，一直以来，阿尔法实验室秉承“攻防一体”的理念，汇聚众多专业技术研究人员，从事攻防技术研究，在安全领域前瞻性技术研究方向上不断前行。作为天融信的安全产品和服务支撑团队，阿尔法实验室精湛的专业技术水平、丰富的排异经验，为天融信产品的研发和升级、承担国家重大安全项目和客户服务提供强有力的技术支撑。

扫描左侧二维码

关注天融信阿尔法实验室公众号