天融信 TOPSEC
证券代码：002212
28

相融共创 赋能未来

2023年
网络空间安全漏洞态势分析研究报告

天融信阿尔法实验室

天融信科技集团

2024年1月

目录

第一章 前言

随着信息技术的迅猛发展和数字化转型的深入推进，网络空间已经成为人们生产、生活、交流不可或缺的重要组成部分。然而，与此同时，网络安全威胁也呈现出前所未有的复杂性和严峻性。安全漏洞，作为网络安全领域的核心问题之一，在这一年中频繁曝光，给全球各地的组织和个人带来了巨大挑战。2023 年，网络空间安全漏洞态势呈现出总体数量降低，但影响范围扩大、利用难度降低的趋势。从传统的系统和应用漏洞，到新兴技术如云计算、物联网、车联网、人工智能等领域的安全隐患，各种类型的安全漏洞层出不穷。这些漏洞不仅威胁着网络系统的正常运行和数据安全，更可能对国家安全、社会稳定和经济发展产生深远影响。

近年来，我们目睹了多起重大的网络安全事件。例如，某知名软件公司的操作系统被发现存在严重的远程代码执行漏洞，攻击者利用该漏洞成功入侵了数百万台计算机，窃取了大量敏感信息。又如，某大型云服务提供商因为配置错误导致客户数据泄露，引发了公众对云安全的广泛关注。这些事件再次提醒我们，网络安全无小事，任何一个看似微小的漏洞都可能成为攻击者的突破口。此外，随着物联网设备的普及和智能化进程的加速推进，物联网安全也成为了一个不容忽视的问题。智能家居设备、智能城市基础设施等物联网设备频繁被曝出存在安全漏洞的情况。这些设备一旦被攻击者控制，不仅可能影响用户的正常生活和工作秩序还可能对用户的隐私和安全造成威胁甚至可能被用于发动更大规模的网络攻击。

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《2023 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 2023 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 2023 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，2022 年共披露漏洞

23900 枚，2023 年共披露漏洞 18635 枚，同比降低 22.03%。这可能表明，在过去一年里，安全运维人员加强了对系统安全的管理，降低了漏洞数量。其中，低危漏洞占 5.85%，中危漏洞占 46.93%，高危漏洞占 47.22%。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 2023 年度高危漏洞预警情况概述,在 2023 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。2023 年度重点漏洞含 Microsoft Word 远程代码执行漏洞、Apache RocketMQ 命令注入漏洞、Atlassian Confluence 远程代码执行漏洞、Linux Kernel 权限提升漏洞等。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。

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。

第二章 国家漏洞库概况

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 2023 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。2023 年来看，漏洞数量出现了持续下降。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，也可能是由于黑客行为的调整。这种波动性提示着网络安全领域的不断演

化和对抗的复杂性。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。

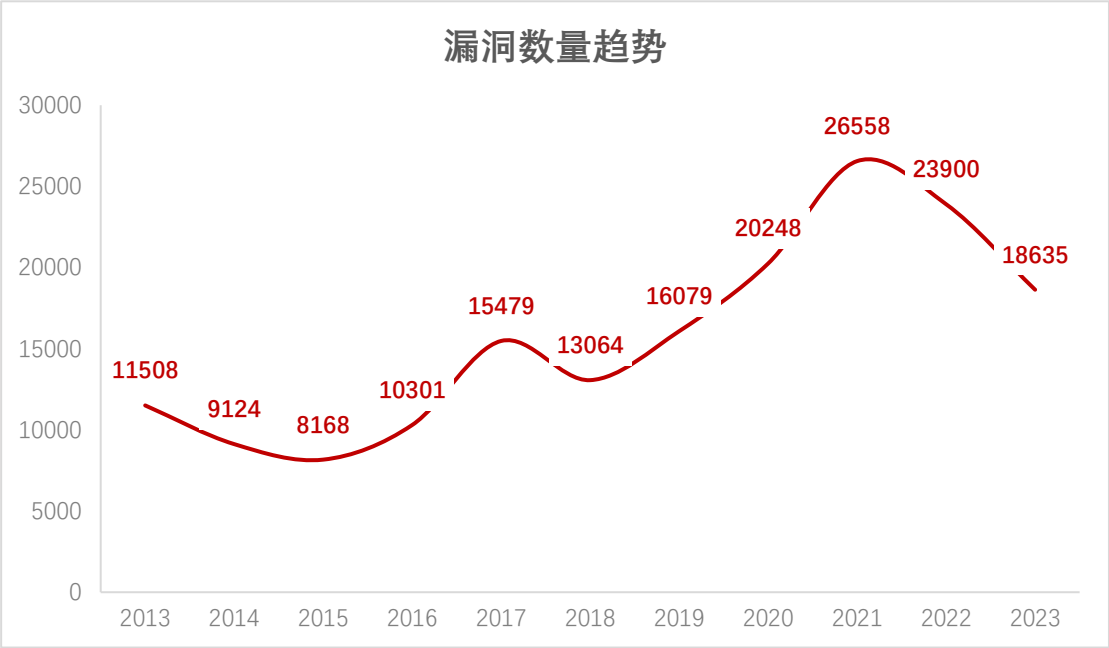

图 1 近十年漏洞数量走势图(数据来自于 CNVD)

2.1 漏洞威胁等级统计

根据 2023 年 1-12 月漏洞引发威胁严重程度统计，其中低危漏洞占 5.85%，中危漏洞占 46.93%，高危漏洞占 47.22%。

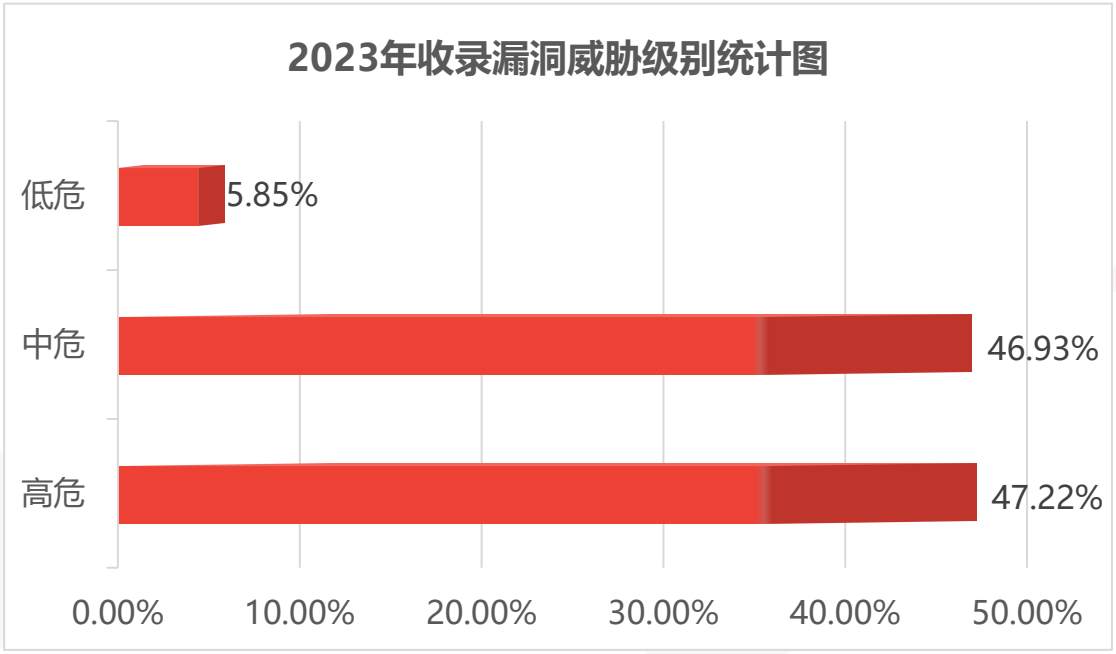

图 2 2023 年收录漏洞按威胁级别统计(数据来自于 CNVD)

分析 2022 年到 2023 年漏洞威胁统计的变化，低危漏洞比例的减少虽然降低了一些噪音，但从实际威胁角度来看确实影响较小，因为这些漏洞的潜在威胁相对较低。然而，中危和高危漏洞比例的上升明显突显了网络安全面临的严峻挑战。中高危漏洞往往具有潜在的严重后果，可能导致数据泄露、系统瘫痪或其他更为严重的安全问题。这趋势提示了安全专业人员需要更加紧密地关注和应对中高危漏洞，采取针对性的安全措施和防护策略，以保障组织在面对复杂多变的网络威胁时的稳健性。

2.2 漏洞影响对象类型统计

根据 2023 年 1-12 月漏洞引发威胁统计，受影响的对象大致可分为八类：分别是 WEB 应用、应用程序、网络设备、操作系统、智能设备、工业控制、安全产品、数据库、车联网系统。其中 WEB 应用漏洞 52.6%，应用程序漏洞 22.8%，网络设备漏洞 14.0%，操作系统漏洞 3.3%，智能设备漏洞 3.2%，工业控制系统漏洞 1.7%，安全产品漏洞 1.5%，数据库系统漏洞 0.7%，车联网系统漏洞 0.2%。

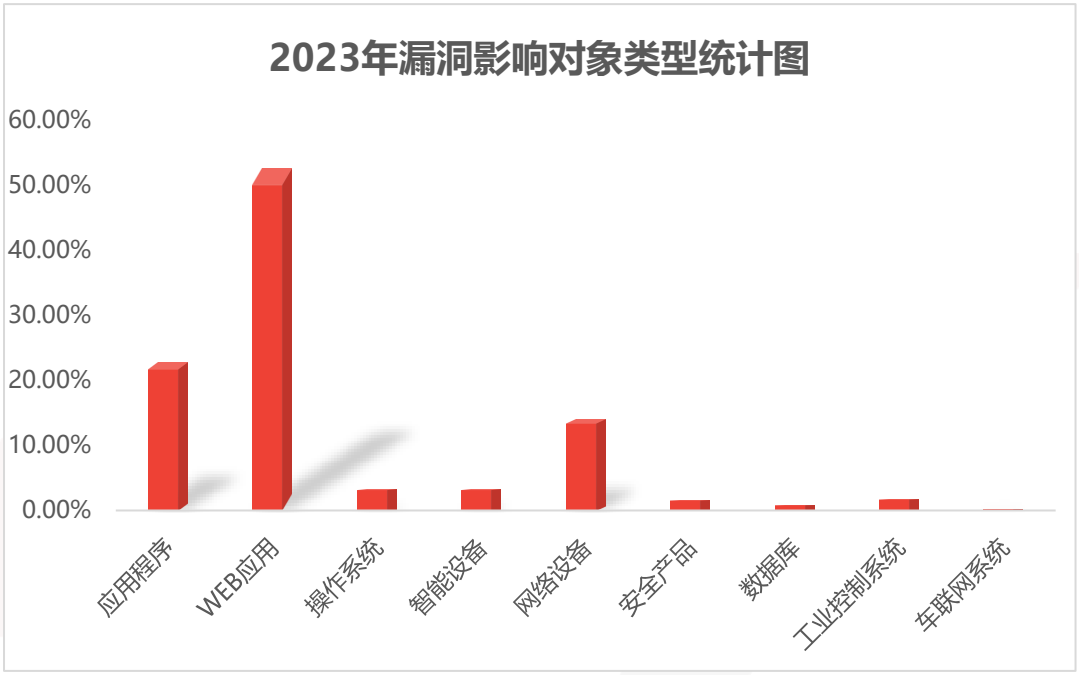

图 3 2023 年漏洞影响对象类型统计(数据来自于 CNVD)

车联网系统漏洞在今年的统计中首次显现，这反映了新能源汽车的崛起对车联网的推动作用。随着新能源技术的迅速发展，汽车制造商在车辆中集成了更多的智能化和联网功能，以提高能源效率、驾驶体验和车辆管理。然而，这也为安全威胁带来了新的挑战，需要对车联网系统的安全性进行更深入的关注和加强。这一趋势突显了新能源技术不仅在环保和科技创新方面发挥着积极作用，同时也对车辆的数字化和联网化提出了新的安全挑战。

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。

2.3 漏洞产生原因统计

根据 2023 年 1-12 月漏洞产生原因的统计，设计错误导致的漏洞占比 67.6% ，屈居首位，紧跟其后的是输入验证错误导致的漏洞占比 28.5%，位居第二，接着是边界条件错误导致的漏洞占比 2.8%，位居第三。后面的访问验证错误、其他错误、竞争错误、意外情况处理错误、配置错误分别占比 0.9%、 0.2%、0.1%、0.01%、0.004%、0.004%。

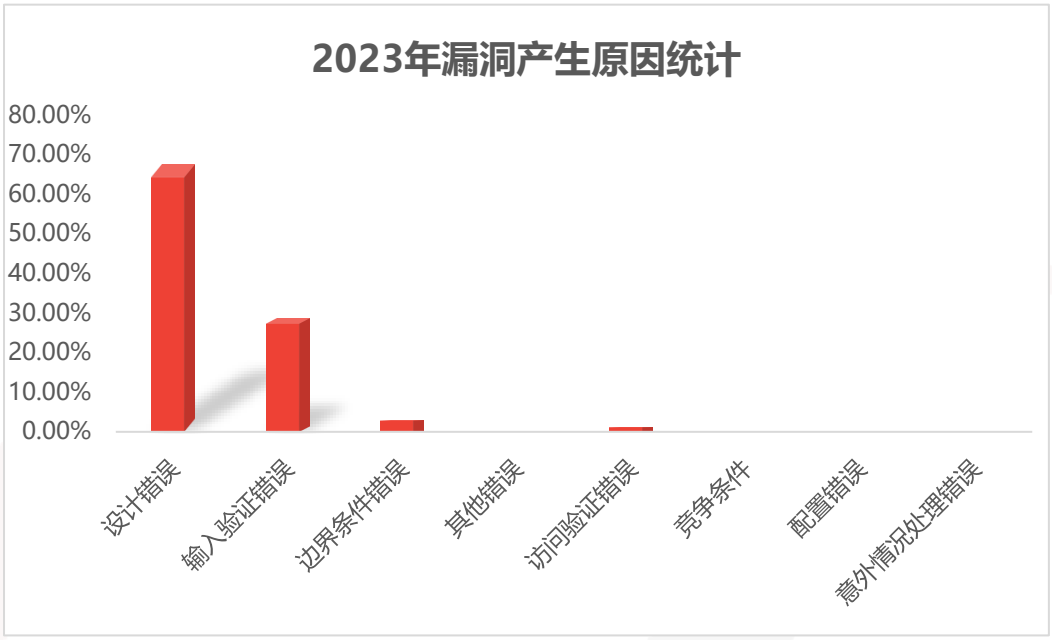

图 4 2023 年漏洞产生原因统计（数据来自于 CNVD）

漏洞的产生原因统计表明，设计错误在导致漏洞的主要原因中居于首位，而这可能反映了在软件开发领域的一种潜在困境。尽管安全开发实践的普及已经在提高，但设计阶段仍然是漏洞频发的根源，这或许意味着在项目早期阶段对于安全性的关注度需要更为强化。此外，输入验证错误紧随其后，揭示了在对用户输入的处理上，一些常见的安全措施可能尚未全面覆盖。这强调了在用户交互方面需要更加深入的安全审查和防范措施。

边界条件错误虽然相对较低，但其出现的频率依然显著，提示着在处理边缘情况时可能存在的漏洞隐患。因此，在开发过程中更加细致入微地考虑输入范围和可能的极端情况是至关重要的。最后，漏洞的根本原因通常与软件开发者对于安全性的认知和培训水平有关，强调了加强安全教育和培训的迫切性，以提高整体开发团队对于潜在风险的敏感性。

2.4 漏洞引发威胁统计

根据 2023 年 1-12 月漏洞引发威胁统计，未授权的信息泄露占比 54.9%居首位，管理员访问权限获取占比 27.7%位居第二，拒绝服务占比 10.0%位居第三，后面的未授权的信息获取、其他、普通用户权限获取。占比分别是 7.1%、0.2%、0.1%。

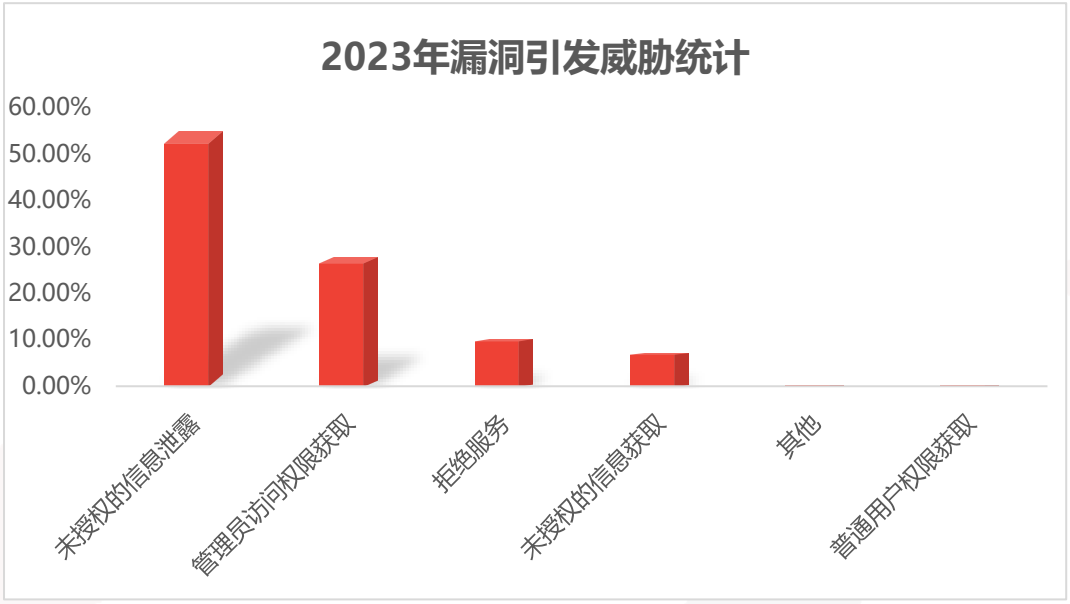

图 5 2023 年漏洞引发威胁统计（数据来自于 CNVD）

在漏洞引发的威胁统计中，未授权的信息泄露呈现持续增长的趋势，凸显了数字时代企业面临的不断演变的风险。这不仅仅是数据泄露的问题，更是对组织信任和声誉的重大挑战。管理员访问权限获取和拒绝服务攻击的占比虽然相对稳定，但未授权信息泄露的激增表明，攻击者越来越善于利用系统的漏洞，直接侵入和窃取敏感信息。

2023 年，随着新一轮科技革命和产业变革的深入发展，中国数据安全产业进入全面快速发展阶段。在数据安全相关机构建设和制度建设日趋完备的“双轮”驱动下，数据安全产业将迎来增长爆发期。天融信作为首批布局数据安全领域的网络安全企业之一，持续探索“数字化安全”新范式，提出了“以数据为中心的安全体系建设”思路，为各行业客户提供体系化的数据安全保障能力。

2023 年是天融信数据安全领域硕果累累的一年，在数据安全场景融合、技术创新、人才培养、奖项成果等方面均取得突破，持续为客户提供优质的数据安全产品和服务。

2.5 行业漏洞收录统计

根据 2023 年 1-12 月行业漏洞统计，2023 年一共收录了电信行业漏洞 1981 枚，移动互联网行业漏洞 1690 枚。工控行业漏洞 422 枚。

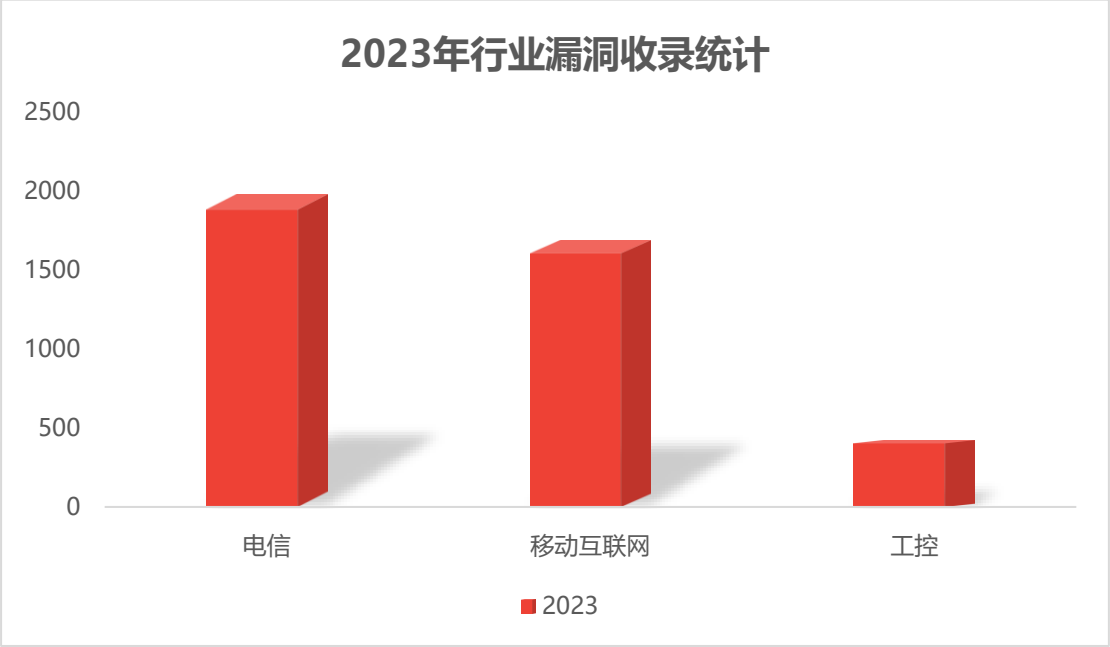

图 6 2023 年行业漏洞收录统计（数据来自 CNVD）

统计显示电信行业和移动互联网行业的漏洞数量相对较高，可能与其复杂的技术体系、庞大的用户基础以及信息流量大等因素有关。表明这两个行业需要更加关注和加强网络安全措施，以确保用户数据和通信的安全性。相比之下，工控行业的漏洞数量较少，这可能是因为工控系统的设备环境和架构较为特殊，使得挖掘漏洞的难度较大。但这也意味着，一旦有人开始关注并挖掘工控系统的漏洞，可能会发现大量的未公开漏洞。随着工业 4.0 的到来，工业控制系统与互联网的连接越来越紧密，这使得工控系统面临着前所未有的网络安全风险。因此，尽管目前工控行业的漏洞数量较少，但我们仍不能对此掉以轻心，需要加强对工控系统的网络安全防护，以防止可能的网络攻击。

2.6 漏洞修复情况统计

根据 2023 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 Oracle、Apple、IBM、Qualcomm、Cisco、Siemens、Dell、ArubaNetworks、NVIDIA 漏洞修复率均为 100%，其余厂商中 Microsoft、Intel、Adobe、Samsung、Google、Linux、WordPress、Fortinet 漏洞修复率分别为 99.91%、99.63%、99.44%、98.54%、98.29%、96.15%、91.74%、81.63%。

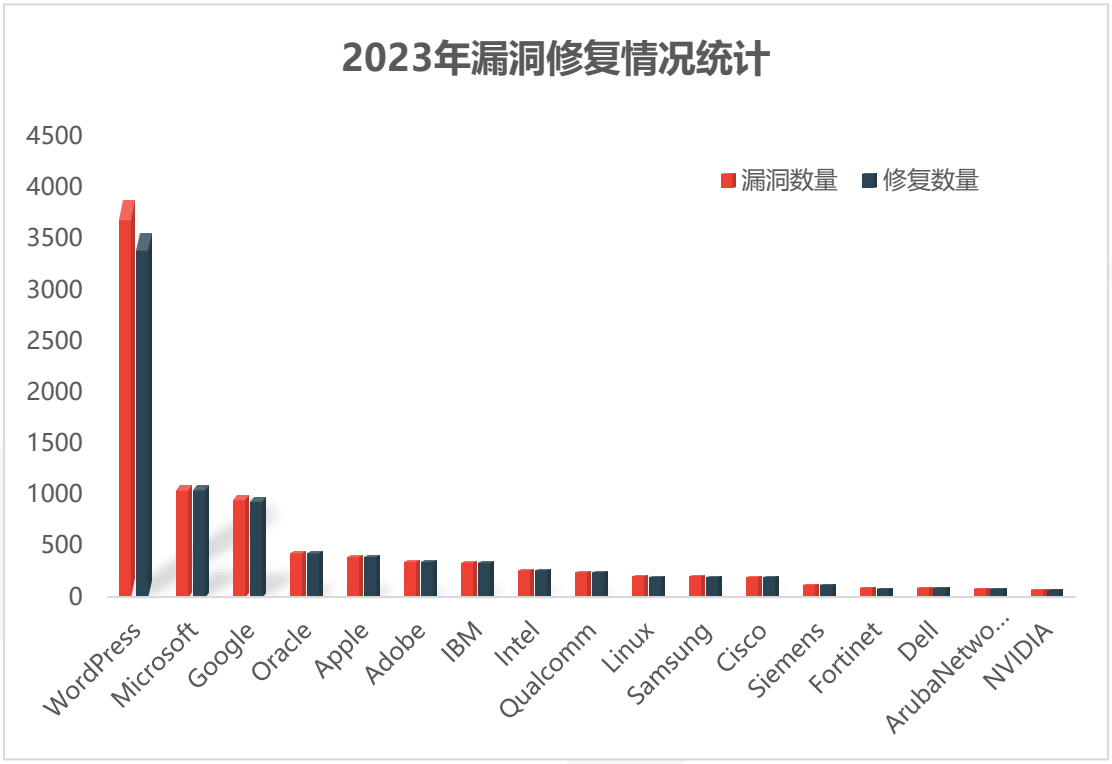

图 7 2023 年漏洞修复情况统计（数据来自 CNNVD）

数据表明大部分厂商在漏洞修复方面表现良好，特别是行业领军企业如 Oracle、Apple、IBM，取得了 100%的修复率，显示了它们对安全性的高度重视。然而，一些知名科技公司仍有提升空间，尤其是在庞大的软件生态系统中漏洞修复较为复杂的情况下。开源项目的漏洞修复率普遍较低，强调建立高效的协作机制的重要性。总体来说，漏洞管理需要全面战略和协同努力，包括不断改进流程、强化安全文化，以确保数字生态系统的可持续安全性。

2.7 漏洞增长趋势

通过 CNVD 漏洞信息库对 2022、2023 漏洞公开数据显示，2022 年一共披露漏洞 23900 枚，2023 年一共披露漏洞 18635 枚。同比减少 22.03%，2022 年高危漏洞 8379 枚，2023 年高危漏洞 8800 枚，同比 2022 年增加 5.02%，2022 年中危漏洞 12862 枚，2023 年中危漏洞 8745 枚，同比 2022 年减少 32.01%，2022 年低危漏洞 2659 枚，2023 年低危漏洞 1090 枚，同比 2022 年减少 59.01%。

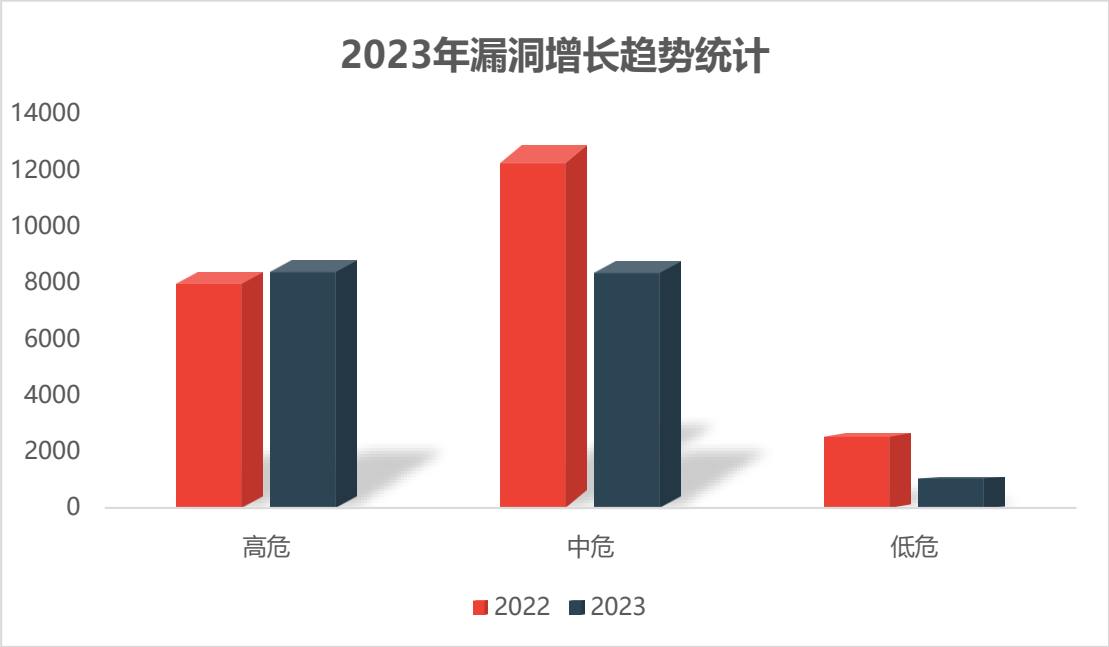

图 8 2023 年漏洞增长趋势统计（数据来自 CNVD）

根据这份数据我们可以看出，高危漏洞在 2022 年至 2023 年有所增加，这可能表明一些安全威胁更加专注于寻找和利用高危漏洞，需要更加紧密的关注。

与此同时，中危漏洞数量在这两年之间发生显著变化，呈现下降趋势。这可能反映了在中危漏洞修复和应对方面，安全社区和企业采取了一些有效的措施。然而，低危漏洞减少的幅度更大，这可能表明对低危威胁的关注度相对较低，或者安全团队更加专注于更为严重的漏洞的修复和预防。

这些趋势强调了动态性和复杂性的漏洞管理，企业需要根据漏洞的特性和威胁情报的变化来灵活调整安全策略。及时修复高危漏洞、注重中危漏洞的防范，以及全面的风险评估将有助于提高整体的安全性。

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 2023 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、Google 及 Apple。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、浏览器、固

件、软件平台、服务器平台其他平台。其中操作系统 31%，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 55%存在未公开 EXP，表明漏洞出现后并不会第一时间发生大规模利用，这就给相关企业留出了一定的缓冲空间。在面临高危漏洞的威胁信息时，需要有一个有效的应急响应计划。包括制定漏洞应急响应流程，建立漏洞应急团队，以及定期进行应急响应的测试和训练，及时防止漏洞带来的各项损失。

从漏洞类型来看，缓冲区溢出、输入验证不当、OS 命令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:

3.1 漏洞影响厂商分布情况

根据 2023 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、Google、Apple。其中 Microsoft 的产品占比达到 17.00%，Google 的产品占到 8.00%，Apple 的产品共占 6.00%。

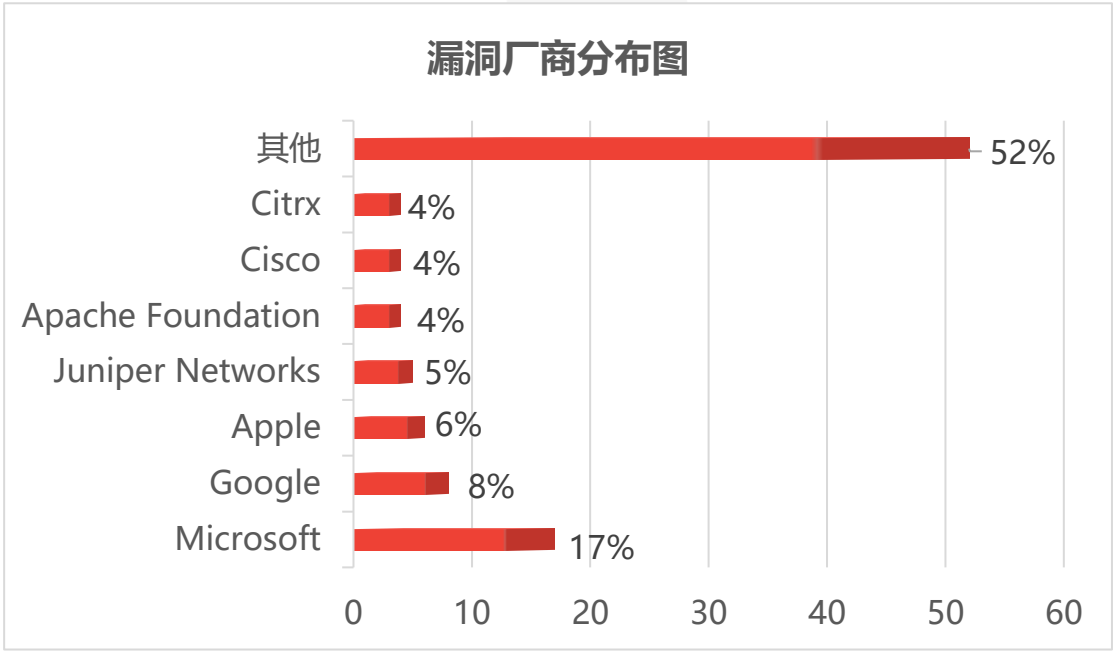

图 9 漏洞厂商分布图(数据来自于 cybersecurity-help)

数据表明微软（Microsoft）受到了最大影响，其个数远超过了其他的公司，因为微软的产品、尤其是操作系统，在全球范围内广泛使用，意味着大量的用户可能被这些安全漏洞影响。谷歌和苹果分别紧随其后，对于这两家公司，尽管披露的数量没有微软那么高，但是由于其在移动设备和互联网服务领域的广泛应用，这些安全漏洞依然可能对大量的用户造成影响。此外，Juniper Networks、Apache Foundation、Cisco 等在网络和基础设施领域的公司也受到了一定程度的影响，强调了整个供应链安全的紧迫性。

3.4 漏洞影响平台产品分类

根据 2023 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、浏览器、固件、软件平台、服务器平台其他平台。其中操作系统 31%、浏览器 6%、固件 6%、软件平台 6%、服务器平台 4%、其他平台 47%。

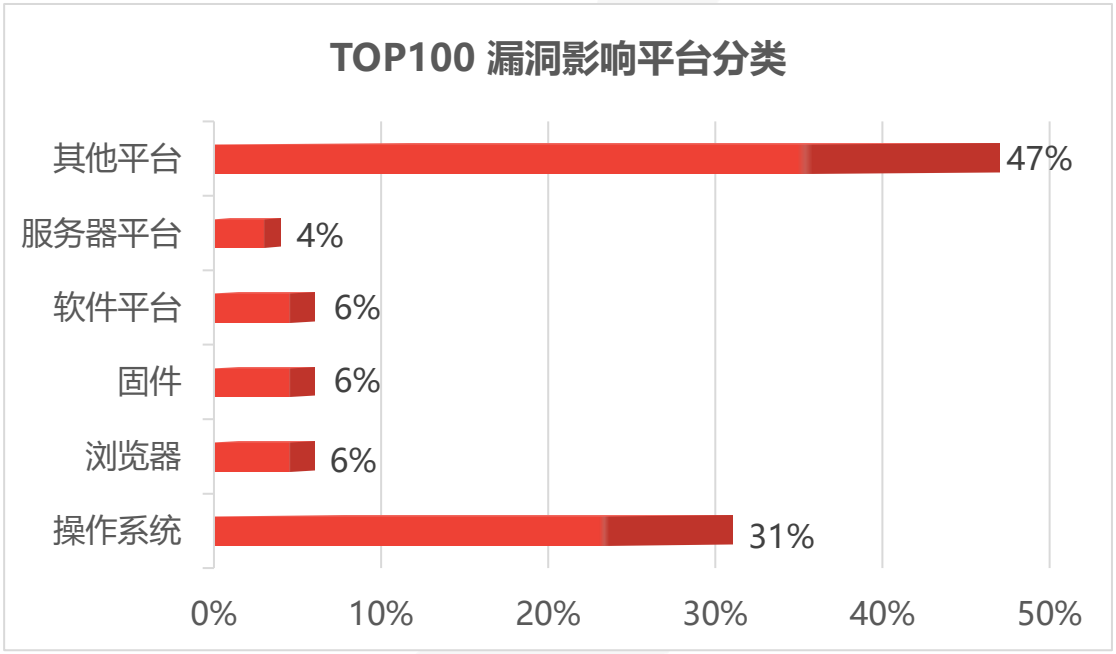

图 10 TOP100 漏洞平台分类(数据来自于 cybersecurity-help)

2023 年的漏洞利用趋势显示，网络安全面临着多样化的挑战。首先，47%的受影响平台归属于“其他平台”，可能包括一些不太常见或专业化的系统或应用，为此我们需要更加关注这些较为边缘的平台，强调对综合性网络安全策略的需求。

在漏洞攻击中，操作系统依然是最主要的受害者，占据了 31%的影响比例。因为大多

数计算设备都依赖于某种操作系统，使其成为黑客攻击的首要目标。相比之下，浏览器和固件的受影响比例较低，或许是因为浏览器广泛采用沙箱技术，而固件在安全性方面的改进也在一定程度上提高了防护水平。

此外，软件平台和服务器平台的影响程度相似，尽管相对较小，但这可能暗示着一些特定的软件和服务器平台在漏洞方面存在相似的风险。这强调了对这些关键基础设施的持续关注和强化安全措施的必要性。

3.5 漏洞类型统计概况

根据 2023 在野利用漏洞前 100 例漏洞类型情况进行统计，其中缓冲区溢出（CWE-119）占比最多，以 13%位居首位，而输入验证不当（CWE-20）占比 10%、OS 命令注入（CWE-78）占比 8%、信息泄露（CWE-200）占比 6%、路径遍历（CWE-22）占比 5%、堆溢出（CWE-122）占比 5%、身份验证绕过（CWE-287）占比 5%、任意文件上传（CWE-434）占比 4%，其他类型占比 44%。

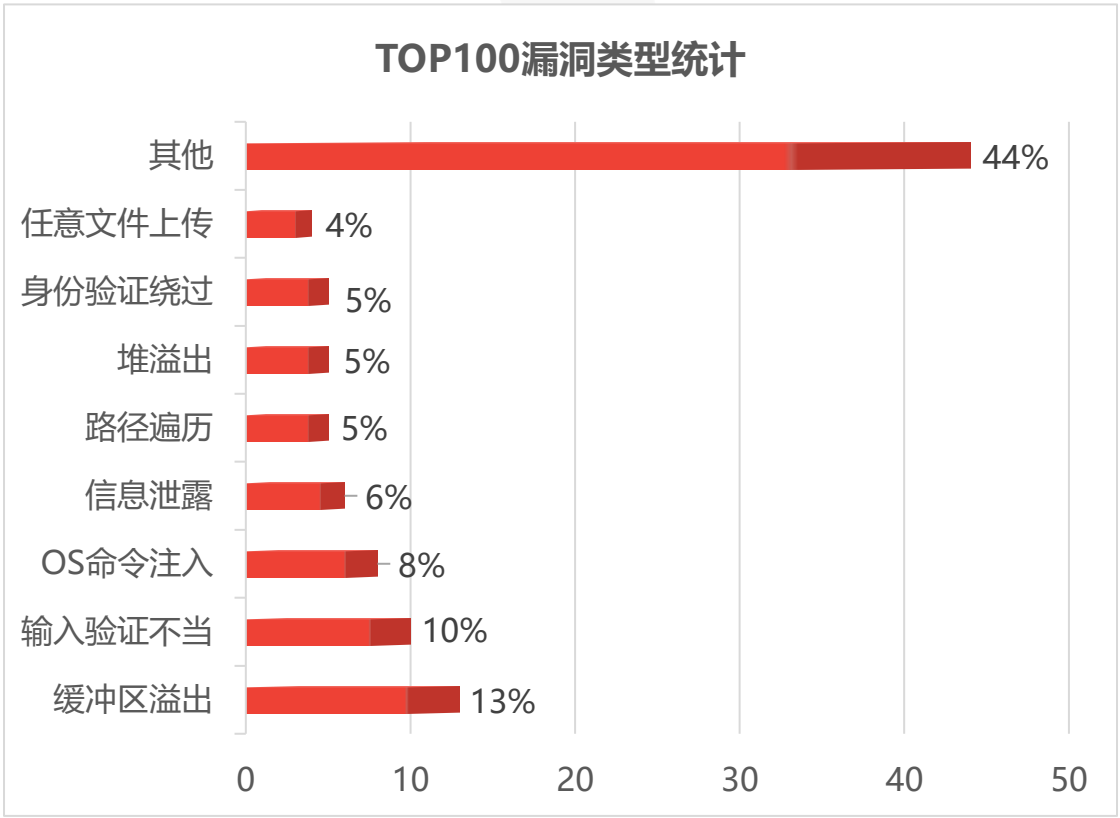

图 11 TOP100 漏洞类型统计概况(数据来自于 cybersecurity-help)

根据 2023 年在野利用漏洞的统计分析，缓冲区溢出被确认为最常见的安全漏洞类型，反映出在软件开发中对数据管理和存储控制的不足，如果没有正确控制缓冲区大小，可能导致恶意代码被执行。紧随其后的是输入验证不当和命令注入，显示了在处理用户输入和系统命令执行时的安全防护措施仍有改进空间。信息泄露、路径遍历、堆溢出、身份验证绕过和任意文件上传等漏洞也相当显著，揭示了在数据保护、访问控制、内存管理和用户身份验证等方面存在的安全隐患。此外，其他各类漏洞占据了较大比例，强调了网络安全威胁的多样性和复杂性。这些统计强调了在各个层面加强网络安全防御和管理的重要性，包括提升安全编码实践、强化配置管理以及提高用户的安全意识。

根据 MITRE 今年通过对公开可用的国家漏洞数据库中 43996 项数据调研分析得出的 CWE TOP 25 排名如下。

排名	ID	名称	分数	与 2022 年排名相比
1	CWE-787	越界写入	63.72	0
2	CWE-79	跨站脚本	45.54	0
3	CWE-89	SQL 注入	34.27	0
4	CWE-416	Use-After-Free	16.71	3
5	CWE-78	OS 命令注入	15.65	1
6	CWE-20	输入验证不当	15.5	-2
7	CWE-125	越界读取	14.6	-2
8	CWE-22	路径遍历	14.11	0
9	CWE-352	跨站请求伪造 (CSRF)	11.73	0
10	CWE-434	危险文件上传	10.41	0
11	CWE-862	缺少授权	6.9	5
12	CWE-476	NULL 指针解引用	6.59	-1
13	CWE-287	身份验证不当	6.39	1
14	CWE-190	整数溢出	5.89	-1
15	CWE-502	反序列化	5.56	-3
16	CWE-77	命令注入	4.95	1
17	CWE-119	缓冲区溢出	4.75	2

18	CWE-798	使用硬编码凭证	4.57	-3
19	CWE-918	服务器端请求伪造 (SSRF)	4.56	2
20	CWE-306	缺少关键功能的身份验证	3.78	-2
21	CWE-362	竞争条件	3.53	1
22	CWE-269	权限管理不当	3.31	7
23	CWE-94	代码注入	3.3	2
24	CWE-863	授权错误	3.16	4
25	CWE-276	不正确的默认权限	3.16	-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-416（Use-After-Free）：从第 7 名提升到第 4 名；

（2） CWE-862（缺少授权）：从第 16 名提升到第 11 名；

（3） CWE-269（权限管理不当）：从第 29 名提升到第 22 名；

（4） CWE-863（授权错误）：从第 28 名提升到第 24 名；

排名大幅下降的漏洞有：

（1） CWE-502（反序列化）：从第 12 名下降到第 15 名；

（2） CWE-798（使用硬编码凭证）：从第 15 名下降到第 18 名；

（3） CWE-276（不正确的默认权限）：从第 20 名下降到第 25 名；

Top 25 中的新入围的漏洞有：

（1） CWE-269（权限管理不当）：从第 29 名上升到第 22 名；

（2） CWE-863（授权错误）：从第 28 名上升到第 24 名；

从 Top 25 中落选的漏洞有：

（1） CWE-400（不受控制的资源消耗）：从第 23 名降至第 37 名；

（2） CWE-611（XML 外部实体引用限制不当）：从第 24 名降至第 28 名；

3.6 EXP 公开情况统计

根据 2023 在野利用漏洞前 100 例 EXP 公开情况进行统计，其中未公开 EXP 稍多，占比 55%，公开 EXP 的为 45%。

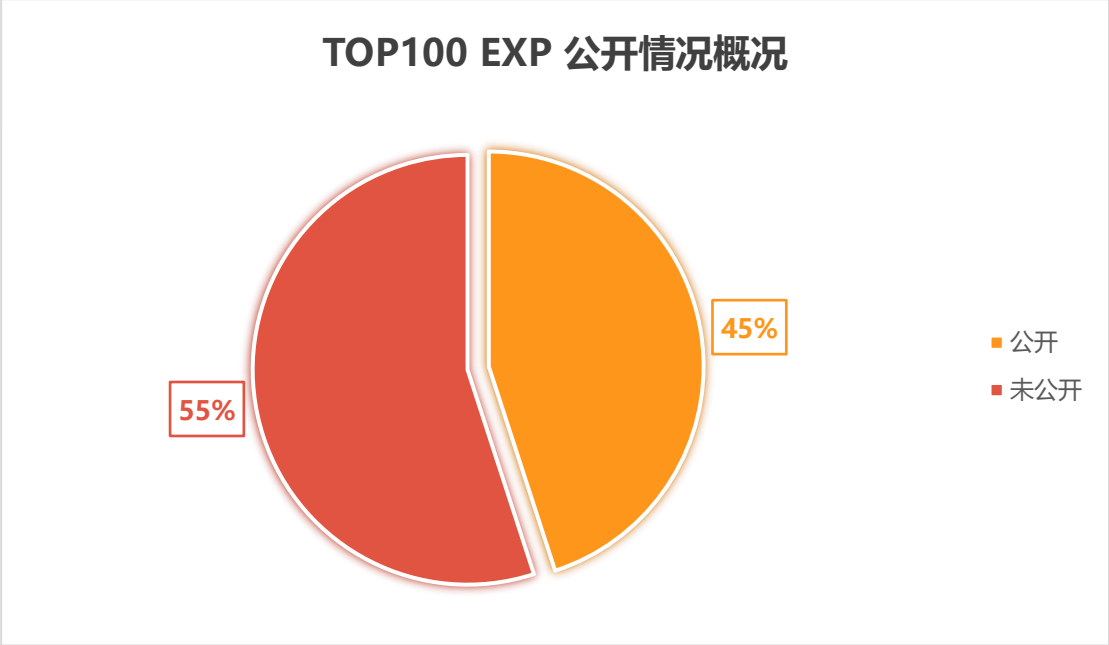

图 12 TOP100 EXP 公开情况概况(数据来自于 cybersecurity-help)

尽管许多公司和研究人员致力于揭示和解决漏洞，但数据表明仍有相当一部分漏洞没有得到公开，这可能会给系统安全带来潜在的威胁。这种现象可能源于多种原因，例如，某些漏洞可能涉及商业秘密，或者由于种种原因，开发人员选择不公开这些漏洞。此外，有些漏洞可能被恶意攻击者利用，他们可能会选择不公开这些漏洞，以便在暗网上出售或共享，从而获取非法利益。

另一方面，公开的漏洞通常是因为已经被发现并报告给了相关的软件供应商或硬件制造商，随后发布了相应的安全更新来修复这些漏洞。总的来说，尽管公开的漏洞数量较少，

但这并不意味着这些漏洞的威胁较小。相反，由于这些漏洞已经被公开，开发人员和安全专家可以利用这些信息来加强安全措施，防止这些漏洞被恶意利用。

第四章 漏洞预警统计情况

2023 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 35762 条，经过漏洞监测系统自动智能筛选后留存高危漏洞信息 361 条，经过人工专家进一步研判后，最终发布了 45 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。2023 年针对 Microsoft 厂商漏洞预警次数达 14 次，其中 Windows 系统的漏洞占大多数。

2023 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 69%。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:

4.1 漏洞厂商情况

在 2023 年内发布的 45 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 14 次，占比约 31%，针对 Apache 的为 5 次，占比 11%，第二名。

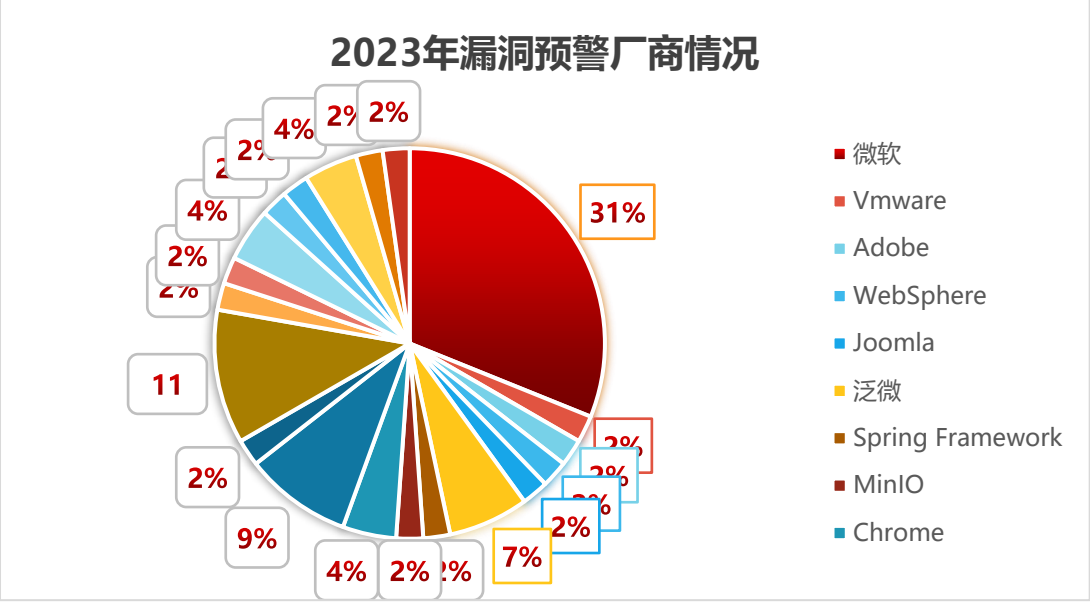

图 13 2023 年漏洞预警厂商情况

从整体情况来看，漏洞通告中涉及众多厂商的产品，微软毫无疑问是这些厂商里面影响力最大的，也正是因为影响力大、使用范围广泛、使用数量众多才会被攻击者高度关注重视，如果攻击者找到微软产品的漏洞，就能获得更多的目标、更大的攻击范围，由于微软产品的复杂性和功能丰富性，使其可能存在潜在漏洞，还有一些早期版本的产品在设计上存在的安全漏洞可能会延续到后续版本中，攻击者更倾向于专门研究微软产品的漏洞，以寻找潜在的攻击机会，并利用这些漏洞来实施网络攻击。同时微软也非常重视自身产品的安全性，依靠安全响应团队监测和应对新的安全威胁，同时通过定期发布安全补丁和更新，以修复产品的漏洞和安全隐患，帮助用户保持系统的安全性。同时，对于使用微软产品的组织或者个人来说，定期更新操作系统和应用程序软件，同时保护自己的个人信息，也应当加强对相关安全知识的学习和掌握，以便在使用过程中尽早发现和处理问题。

众多厂商的产品出现安全漏洞通常是由于多种原因造成的。产品的复杂性使得漏洞更容易隐藏在代码中，难以被完全发现和修复。此外，产品需要连接到网络或其他设备，增加了受到攻击的可能性。设计缺陷、用户输入和管理问题也可能导致安全漏洞的产生。人为因素和人为错误也是安全威胁的常见来源。

国内的安全爱好者也会特别关注国产的内容管理系统（CMS）和办公自动化（OA）软件，因为这些软件在企业和政府机构中广泛使用。这些系统涉及大量敏感信息和数据，如客户数据、财务信息等。一旦这些软件遭受攻击或泄露，可能会对企业和用户造成严重损失。此外，关注国产软件的安全性也有助于提升国内软件安全水平，促进本土软件产业的发展和创新。

4.2 漏洞威胁情况

在 2023 年发布的 45 条漏洞通告中，所通告的漏洞可分为 9 大类，分别是远程代码执行漏洞、权限提升漏洞、文件上传漏洞、认证绕过漏洞、SQL 注入漏洞、敏感信息泄露漏洞、任意文件读取漏洞、命令注入漏洞、缓冲区溢出漏洞，其中远程代码执行漏洞占比 69%，位于首位，权限提升漏洞、文件上传漏洞、认证绕过漏洞占比 7%，并列位于第二位。

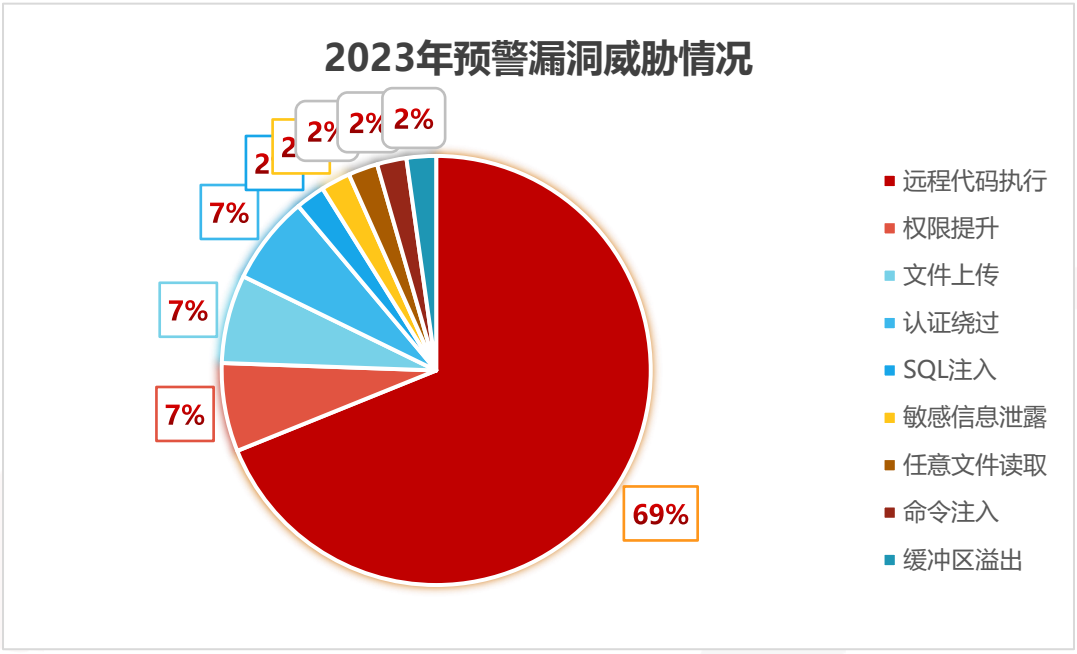

图 14 2023 年预警漏洞威胁情况

由此可见，随着网络安全技术的发展，攻击者们越来越倾向于利用代码执行漏洞来获取服务器权限，进而实现攻击目的。其次是权限提升漏洞、认证验证绕过漏洞和文件上传漏洞，权限提升漏洞允许攻击者在没有正确授权的情况下获得系统或软件的高级权限，可能导致数据泄露或其他严重后果。认证验证绕过漏洞可以让攻击者绕过身份验证机制，获取未授权的访问权限。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，敏感信息泄露漏洞、SQL 注入漏洞、命令注入漏洞、缓冲区溢出和任意文件读取漏洞的比例都较低，但仍需引起重视。敏感信息泄露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，命令注入漏洞可能允许攻击者在系统中执行任意命令，缓冲区溢出漏洞受影响的程序输入超出其预期大小的数据，从而覆盖相邻内存区域，甚至执行恶意代码或者系统崩溃，任意文件读取漏洞读取漏洞获取服务器上的敏感信息，如配置文件、用户凭证、日志文件等。因此应该继续加强安全意识，不断更新防护措施。

4.3 年度 TOP10 高危漏洞

本节内容筛选自天融信 2023 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-2023-21716	Microsoft Word 远程代码执行漏洞	CVE-2023-21716：未经身份验证的攻击者可能会发送包含 RTF 有效负载的恶意电子邮件，这将使他们能够获得在用于打开恶意文件的应用程序中执行命令的访问权限。
NO.2	CVE-2023-33246	Apache RocketMQ 命令注入漏洞	CVE-2023-33246 ：RocketMQ 的 NameServer、Broker、Controller 等多个组件暴露在外网且缺乏权限验证，攻击者可以利用此漏洞以 RocketMQ 运行的系统用户身份执行命令。
NO.3	CVE-2023-22518	Atlassian Confluence 远程代码执行漏洞	CVE-2023-22518 ： Confluence 滥用了 Struts2 的继承关系，从而导致可以一定程度绕过它自身的权限校验，最终通过部分接口串联利用实现无需认证的远程代码执行。
NO.4	CVE-2023-3269	Linux Kernel 权限提升漏洞	CVE-2023-3269：Linux 内核的内存管理子系统存在释放后重用漏洞，低权限用户可以利用此漏洞提升至 ROOT 权限。
NO.5	CVE-2023-3519	Citrix ADC 及 Citrix Gateway 远程代码执行漏洞	当 Citrix ADC 或 Citrix Gateway 设备配置为网关（VPN 虚拟服务器、ICA 代理、CVPN、RDP 代理）或 AAA 虚拟服务器时，未经身份验证的远程威胁者可利用该漏洞在目标设备上执行任意代码。
NO.6	CVE-2022-41678	Apache ActiveMQ Jolokia 代码执行漏洞	经过身份验证的恶意攻击者通过/api/jolokia/接口来操作 MBean，成功利用此漏洞可在目标服务器上执行任意代码，获取目标服务器的控制权限。
NO.7	CVE-2023-50164	Apache Struts2 文件上传漏洞	CVE-2023-50164：漏洞源于上传文件参数名的大小写校验存在问题，从而使得通过特定参数名来指定文件名实现目录遍历上传恶意文件，未经授权的攻击者可能利用这个漏洞上传恶意文件到服务器并执行任意代码。

NO.8	CVE-2023-38646	Metabase 远程命令执行漏洞	CVE-2023-38646：Metabase 中支持嵌入式内存数据库 H2，由于连接数据库时过滤不严，可通过 H2 JDBC 连接导致命令执行，成功利用该漏洞可在 Metabase 服务器上远程执行代码。
NO.9	CVE-2023-20860	Spring Framework 身份认证绕过漏洞	Spring Framework 存在一处身份认证绕过漏洞，当 Spring Security 配置中用作"**"模式时，会导致 Spring Security 和 Spring MVC 之间的 mvcRequestMatcher 模式不匹配。允许未经身份验证的远程攻击者通过向目标发送构造的特制请求，实现身份验证绕过，进而访问后台信息。
NO.10	CVE-2023-37582	Apache RocketMQ 远程代码执行漏洞	CVE-2023-37582：此漏洞是由于 CVE-2023-33246 补丁未修复完全，当 RocketMQ 的 NameServer 组件暴露在外网，且缺乏有效的身份认证时，攻击者可以利用更新配置功能，以 RocketMQ 运行的系统用户身份执行任意命令。

表 2 TOP10 危害排名

4.4 漏洞预警 TOP10 漏洞回顾

一、Microsoft Word 远程代码执行漏洞
漏洞类型：远程代码执行 漏洞编号：CVE-2023-21716 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：2023-4-7 漏洞描述：CVE-2023-21716 是 Microsoft Word 的 RTF 解析器（wwlib）中的一个远程代码执行漏洞。攻击者可以通过制作包含大量字体表项的 RTF 文档，并向目标用户发送邮件，

诱导用户打开邮件中包含的恶意文档。攻击者可利用多种方式诱导用户打开恶意的 RTF 文档，如电子邮件、即时消息等等。Windows 文件浏览器和 Microsoft Outlook 的预览窗格都可以作为此漏洞的攻击媒介。成功利用此漏洞，可使攻击者获得在目标系统上以当前用户的权限执行任意代码的能力。

二、Apache RocketMQ 命令注入漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2023-33246

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：2023-6-5

漏洞描述：对于 RocketMQ 5.1.0 及以下版本，在某些条件下，存在远程命令执行的风险。RocketMQ 的 NameServer、Broker、Controller 等多个组件存在外网泄露且缺乏权限验证，攻击者可以通过更新配置功能以 RocketMQ 运行的系统用户身份执行命令来利用该漏洞。此外，攻击者还可以通过伪造 RocketMQ 协议内容来达到同样的效果。为了防止此类攻击，建议用户使用 RocketMQ 5.x 时升级到 5.1.1 或以上版本，使用 RocketMQ 4.x 时建议升级到 4.9.6 或以上版本。

三、Atlassian Confluence 远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2022-22965

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：2023-11-1

漏洞描述：Confluence Data Center 和 Server 的所有版本均受此未利用漏洞的影响。此不当授权漏洞允许未经身份验证的攻击者重置 Confluence 并创建 Confluence 实例管理员帐户。使用此帐户，攻击者可以执行 Confluence 实例管理员可用的所有管理操作，从而导致（但不限于）完全丧失机密性、完整性和可用性。Atlassian Cloud 站点不受此漏洞的影响。如果您的 Confluence 站点是通过 atlassian.net 域访问的，则该站点由 Atlassian 托管，并且不易受到此问题的影响。

四、Linux Kernel 权限提升漏洞

漏洞类型：权限提升

漏洞编号：CVE-2023-3269

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

漏洞评分：7.8

预警日期：2023-8-2

漏洞描述：Linux 内核的内存管理子系统中存在漏洞。访问和更新虚拟内存区域（VMA）的锁处理不正确，导致释放后使用问题。该问题可被成功利用来执行任意内核代码、升级容器并获取 root 权限。该漏洞是由于 Chrome V8 引擎中存在类型混淆所导致，此类漏洞通常会在成功读取或写入超出缓冲区边界的内存后造成浏览器崩溃或者执行任意代码。影响范围：Chrome for Mac/Linux < 107.0.5304.87 、Chrome for Windows < 107.0.5304.87。

五、Citrix ADC 及 Citrix Gateway 远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2023-3519

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：2023-7-27

漏洞描述：Citrix ADC 是一种应用交付控制器，用于提高应用性能、安全性和可靠性。它是一种强大的应用交付平台，具有多种功能，旨在优化应用程序交付、负载均衡和安全性。Citrix Gateway 是 Citrix ADC 的一部分，为用户提供安全的远程访问到企业网络和应用程序的能力。它提供了安全的远程连接和访问控制，让用户可以通过安全的通道（通常是 SSL/TLS 加密）从远程位置连接到公司网络，访问内部资源和应用程序，同时确保数据传输的安全性和隐私。CVE-2023-3519 该漏洞是当 Citrix ADC 或 Citrix Gateway 设备配置为网关（VPN 虚拟服务器、ICA 代理、CVPN、RDP 代理）或 AAA 虚拟服务器时，未经身份验证的远程威胁者可利用该漏洞在目标设备上执行任意代码。

六、Apache ActiveMQ Jolokia 代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2022-41678

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：2023-11-30

漏洞描述：一旦用户在 Jolokia 上通过身份验证，他就有可能触发任意代码执行。具体来说，在 ActiveMQ 配置中，jetty 允许 org.jolokia.http.AgentServlet 处理对 /api/jolokia 的请求。org.jolokia.http.HttpRequestHandler#handlePostRequest 能够通过 JSONObject 创建 JmxRequest。并调用 org.jolokia.http.HttpRequestHandler#executeRequest。进入更深的调用栈，

org.jolokia.handler.ExecHandler#doHandleRequest 可以通过反射来调用。可以通过 Java 版本 11 以上的 jdk.management.jfr.FlightRecorderMXBeanImpl 来实现 RCE。 1 调用 newRecording。2 调用 setConfiguration。其中隐藏着一个 webshell 数据。3 调用开始录音。4 调用 copyTo 方法。Webshell 将写入 .jsp 文件。缓解措施是限制（默认情况下）Jolokia 上授权的操作，或禁用 Jolokia。默认 ActiveMQ 发行版中定义了更具限制性的 Jolokia 配置。我们鼓励用户升级到 ActiveMQ 发行版本，包括更新的 Jolokia 配置：5.16.6、5.17.4、5.18.0、6.0.0。

七、Apache Struts2 文件上传漏洞

漏洞类型：文件上传漏洞

漏洞编号：CVE-2023-50164

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：2023-12-11

漏洞描述：Apache Struts 广泛集成到各种系统中，并因 2017 年臭名昭著的 Equifax 漏洞而引起了广泛关注。Equifax 漏洞影响了超过 1.45 亿人，并导致消费者信用报告机构支付了 7 亿美元的和解金。该事件的一个重要方面涉及 Equifax 黑客在一次大规模攻击中窃取了 200,000 个信用卡账户。Apache Software Foundation 发布了安全性更新，以应对 Struts 2 开源框架中的关键文件上传漏洞。成功利用该漏洞（跟踪为 CVE-2023-50164）可导致远程代码执行。建议用户应立即升级到 Struts 2.5.33 或 Struts 6.3.0.2 或更高版本。

八、Metabase 远程命令执行漏洞

漏洞类型：远程命令执行

漏洞编号：CVE-2023-37470

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：2023-7-27

漏洞描述：Metabase 是一个开源的数据分析和可视化工具，旨在让非技术人员能够轻松地通过直观的界面探索和理解数据。它提供了一个直观的用户界面，允许用户直接连接到各种数据源（如数据库、CSV 文件等），进行数据查询、可视化和共享分析结果。0.46.6.1 之前的开源 Metabase 和 1.46.6.1 之前的 Metabase Enterprise 允许攻击者以服务器的权限级别在服务器上执行任意命令。利用时不需要身份验证。

九、Spring Framework 身份认证绕过漏洞

漏洞类型：身份认证绕过

漏洞编号：CVE-2023-20860

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

漏洞评分：7.5

预警日期：2023-4-7

漏洞描述：Spring Framework 是一个轻量级的开源 Java 框架，旨在简化企业级应用程序的开发。它提供了一组全面的功能，例如依赖注入、面向切面编程、模板模式、JDBC 模板、Hibernate 模板、事务管理等，可以帮助开发人员编写高质量、可维护的代码。Spring 框架还提供了许多扩展框架，例如 Spring MVC、Spring Security、Spring Data、Spring Batch 等等，可以帮助开发人员更快速地构建和部署各种类型的应用程序。Spring Framework 被广泛应用于企业级 Java 应用程序的开发。运行版本 6.0.0 - 6.0.6 或 5.3.0 - 5.3.25 的 Spring Framework 在带有 mvcRequestMatcher 的 Spring Security 配置中使用“**”作为模式会导致 Spring Security 和 Spring MVC 之间的模

式匹配不匹配，并且可能用于安全绕过。

十、Apache RocketMQ 远程代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2023-37582

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：2023-7-18

漏洞描述：Apache RocketMQ 是一个开源的分布式消息队列系统，具有高吞吐量、低延迟和高可靠性的特点。它采用分布式架构，支持横向扩展和高可用性，能够处理大规模分布式系统的消息通信需求。RocketMQ 提供灵活的消息模型，支持发布/订阅和点对点模式，以满足不同的应用场景。它具有消息过滤、顺序传递和实时监控等功能，并具备良好的可扩展性和兼容性。作为一种可靠的消息中间件，RocketMQ 被广泛应用于实时消息传递、异步处理和事件驱动架构等场景，帮助构建高性能、可扩展和可靠的分布式应用系统。RocketMQ NameServer 组件仍然存在远程命令执行漏洞，CVE-2023-33246 问题在 5.1.1 版本中尚未完全修复。当 NameServer 地址在外网泄露且缺乏权限验证时，攻击者可以利用该漏洞，通过 NameServer 组件上的更新配置功能，以 RocketMQ 运行的系统用户身份执行命令。建议用户将 NameServer 版本升级到 RocketMQ 5.x 的 5.1.2 或更高版本，或者 RocketMQ 4.x 的 NameServer 版本升级到 4.9.7 或更高版本，以防止这些攻击。

第五章 总结

2023 年网络空间安全漏洞态势分析研究报告显示，漏洞数据总数呈现下降趋势，但高危漏洞数量仍然为增长态势。我们需要从两个方面进行思考：首先，总体漏洞数量的下降

可能意味着安全技术的不断进步和漏洞管理的改善，例如更多的漏洞被发现并在披露后得到修复。这是一个积极的趋势，表明安全领域正在不断发展和进步。然而，高危漏洞数量的增长则需要我们更加投入关注和积极处理。高危漏洞的存在带来了更大的安全风险，因为它们更倾向被攻击者利用。高危漏洞的增长可能反映出当前的安全技术无法有效地防止或快速修复这些漏洞，或者新的威胁模式和技术正在出现。

通过对 2023 年前 100 个在野利用漏洞统计看出，Microsoft、Google 和 Apple 为主要攻击目标，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。操作系统的漏洞占据首位，55%的漏洞存在未公开 EXP，强调了操作系统安全性的脆弱性。最严峻的威胁来自缓冲区溢出、输入验证不当和 OS 命令注入等漏洞类型。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。

2023 年漏洞预警显示，主流操作系统成为漏洞高发的产品类别。Microsoft 厂商在漏洞预警中的突出地位反映了其产品在市场上的广泛使用和由此带来的潜在风险。尤其是 Windows 系统的漏洞频繁出现，凸显了对操作系统安全性的持续关注和改进需求。远程代码执行漏洞的高占比是一个值得关注的趋势，这类漏洞由于其高度的破坏性和隐蔽性，一直是 APT 攻击者的主要攻击手段。这要求企业在网络安全策略中加大对这类漏洞的防御力度，包括定期更新系统和应用程序、实施严格的访问控制以及采用先进的威胁检测和响应技术。针对知名厂商的漏洞预警分布情况，微软和 Apache 占据了显著比例，这指示了在选择和使用第三方软件产品时，企业应特别关注这些厂商的安全更新和漏洞管理实践。同时，这也为企业在供应链安全管理和供应商评估方面提供了重要参考。

5.1 安全防护建议

在归纳 2023 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.实施严格的供应商审查机制，防范供应链攻击：随着企业业务的扩展，对外部供应商的依赖程度逐渐加深，供应链攻击的风险也随之增加。这类攻击可能来自第三方软件、硬件或者服务，一旦攻击成功，可能会造成重要数据的泄露、系统的瘫痪等严重后果。为

了应对这种威胁，企业需要实施严格的供应商审查机制，包括对供应商的网络安全能力、过往的安全记录等进行全面评估。同时，采用零信任网络架构，对所有进出网络的数据和流量进行严格控制和检测，防止恶意软件和未经授权的访问。

2.加强账户安全，避免身份和凭证欺诈：随着数字化转型的加速，身份和凭证欺诈成为一种日益严重的威胁。攻击者通过窃取个人信息和登录凭证，冒充受害者进行非法访问和交易。为了应对这种威胁，企业和个人应加强账户安全，使用强密码和多因素身份验证，定期更改密码，以及避免在非官方应用中使用个人信息。

3.建立系统的漏洞管理体系，以应对安全漏洞威胁：网络安全是动态的而不是静态的，应重视信息系统的安全性，进一步加大安全投入。从源头的厂商看起，应为研发提供足够的资源支持，在系统的规划、设计、实现、测试、维护等全生命周期内嵌入安全基因，设立并力求形成统一且全面的安全性能目标，避免系统的各项安全指标和总体安全性处于孤立、片面或是有限的局面，进而形成致命的安全漏洞；在政企单位等组织一侧，数字化为日常工作带来了极大的便利性，但动态的安全运维工作同样不可轻视，应设立大小匹配的专职安全岗位，建立和实施具体、细致且长期持续的安全运维方案。为防止各类突发事件的风险，还需建立风险应急预案及安全管理储备；对于个人普通用户而言，较之重点目标通常不是第一攻击对象，但安全是整体的，个体组合形成整体，个体安全被突破意味着整体安全存在被突破的风险。故此，为避免因个人用户带来的风险，减少攻击面加强安全意识实为重中之重。

4.增强分段网络管理，强化数据安全应对能力：随着数字化转型的加速，企业的数据量呈现爆炸性增长，数据安全风险也随之增加。为了应对这种风险，企业需要建立完善的数据产权结构性分置制度，明确数据的所有权、使用权、收益权等。同时，加强数据安全治理也是非常重要的，包括建立数据分类分级制度、制定严格的数据使用和访问控制策略等。此外，定期进行数据安全审计和风险评估也是必不可少的。2023 年 10 月下旬，波音公司遭遇 LockBit 勒索软件攻击，LockBit 在数据泄露站点发消息声称窃取了波音的大量敏感数据，并以此胁迫波音公司，如果不在 2023 年 11 月 2 日前与 LockBit 组织取得联系，将会公开窃取到的敏感数据。从这起事件可以看出，利用漏洞植入勒索软件进而窃取关键数据的事件危害巨大，需要增强网络分段管理，提升数据安全。采取有效的网络分段，以

限制漏洞的影响范围，并减少漏洞利用成功的潜在影响，以达到提升数据安全的目标。网络分段有助于限制漏洞的范围，减少漏洞利用的潜在影响。通过将网络划分为独立的子网，甚至完全独立的物理网络，保护敏感数据免受未经授权的访问，或是因网络攻击造成大范围泄露。

天融信积极响应数智时代的发展趋势，以“以数据为中心的安全架构”为基础，从体系研究、技术创新、产品研发、安全服务、人才培养等多维度推进数据安全体系化建设。其获得的国家信息安全服务数据安全类一级资质进一步证实了其在数据安全领域的实力。

最近，国家数据局发布了《“数据要素×”三年行动计划（2024—2026 年）（征求意见稿）》，旨在促进我国数据基础资源优势转化为经济发展新优势。天融信与国家发展步伐同频共振，充分发挥网络安全领军企业的作用，提升企业数据安全保障水平，为经济社会发展赋能。

5.2 2024 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。2024 年，预计将有几个关键趋势影响着漏洞的发展、利用、防御以及监测预警。

漏洞发展的趋势显示，零日漏洞的利用将继续增长，特别是国家级黑客组织和网络犯罪团伙会更多地使用这些漏洞，以便实现对攻击目标的长久控制。新兴技术领域成为重点攻击对象：云计算、物联网、车联网、人工智能等新兴技术将继续成为安全漏洞的重点领域。例如，随着 5G 网络的普及和边缘计算的广泛应用，与之相关的安全漏洞可能会逐渐增多。同时，人工智能和机器学习技术的发展也将带来新的安全挑战，如数据泄露、模型篡改等。

在漏洞利用方面，勒索软件攻击将变得更有针对性和狡猾，攻击者将重点攻击关键基础设施和高价值目标。随着生成式人工智能（GAI）技术的快速发展，可能会看到更复杂、更智能的网络攻击。GAI 的出现使得人工智能不仅被用于漏洞防御，还可能被恶意应用于攻击策略的设计和执行，大大降低攻击者的攻击门槛。

在漏洞防御方面，重点关注开源软件，因为开源软件几乎渗透在每一个角落，支撑着

广泛的领域，包括但不限于网络服务器的运行、操作系统的运作，乃至移动应用程序的开发和云服务的提供。开源生态系统的相互关联性意味着一个单一的漏洞有可能引发连锁反应，这种反应能够从一个应用程序蔓延到另一个应用程序，并且有可能对大量系统和用户造成影响。预计到 2024 年，开源软件会增加对安全审查的投入，软件安全的“左移”策略，即在开发的早期阶段就整合安全考虑，有望在开源软件中继续保持其发展势头，并贯穿全年。专注于开源安全的专业团队数量预计将显著增加。随着对供应链完整性和透明度的关注度提高，开源生态系统中确保供应链安全的需求预计会进一步增强。同时，预计开源社区内的协作将会加强，推动以社区为导向的安全计划增长。开源软件的安全性可能会成为更加核心的关注点，尤其是考虑到其在数字基础设施中持续发挥关键作用。因此，对开源软件进行监管的必要性和重要性将变得更加明显，并可能成为未来发展的重点。随着网络攻击的频率和复杂性不断提高，传统网络安全工具和方法逐渐失效，零信任架构成为了解决持续网络安全问题的首选安全框架，并将是未来漏洞防御的重要趋势。虽然目前只有少数组织完全符合零信任架构的要求，但随着网络安全环境的不断变化，越来越多的组织将开始采用零信任架构，以提高网络安全防护能力。

对于漏洞监测预警，人工智能（AI）将成为实时网络安全漏洞识别和防护的关键技术。AI 将能够自动学习识别、预测潜在风险和威胁，并自动隔离这些风险，实现比人更快、更好、更准确的实时识别和快速反应。随着攻击者利用 AI 和其他先进技术，防御者也必须采用更先进的技术和策略来保护自己的网络安全。包括投资 AI 和机器学习技术，以及加强员工培训和事件响应计划。组织会增加对主动安全工具和技术的投资，以更好地发现漏洞和安全问题，以满足其特定需求。这包括基于风险的漏洞管理、攻击面管理、适用于应用程序、云和数据的安全态势工具，以及攻击路径管理和安全控制验证，如渗透测试、红队演练和攻击模拟等方面的考虑。此外，随着 IAST（交互式应用程序安全测试）技术的不断成熟和普及，组织正逐渐将其整合到全链路接口安全防御体系中，实现对应用安全漏洞的实时、深度检测和响应。借助插桩技术动态监测运行时数据流，IAST 能追踪敏感信息在接口调用链中的流动与处理，提供准确及时的安全威胁告警，并结合自动化验证与 DevSecOps 流程促进安全问题的快速修复。覆盖整个应用生命周期且适应云环境变化，IAST 强化了跨层级、全方位的接口安全防护能力。

为了应对未来一年中的网络安全挑战，政府、企业和个人需要加强合作与信息共享，

共同构建一个更加安全的网络空间。同时，也需要加强技术研发和人才培养，提升自身的网络安全能力和水平。只有这样，才能在新的一年中更好地应对各种网络安全威胁和挑战。

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。

天融信还专注于强化云端情报融合、安全防护设备联动、云环境下的 IT 资产安全管理等能力，将云上能力赋能本地，结合云端 7×24 小时在线研判，帮助各类客户构建涵盖检测发现、分析研判、情报预警、响应处置、持续监控的完整资产安全管理体系。使得客户的数字化转型发展更加顺利，并在数字化转型过程中得到有力的保驾护航。

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。