天融信 TOPSEC
证券代码：002212
27th

相融共创 赋能未来

# 2022年
# 网络空间安全漏洞分析研究报告

天融信阿尔法实验室

天融信科技集团

2023年1月

# 目录

第一章 前言 ..... 3
第二章 CNVD 漏洞库安全漏洞概况 ..... 5
2.1 漏洞威胁等级统计 ..... 5
2.2 漏洞利用攻击位置统计 ..... 6
2.3 漏洞影响对象类型统计 ..... 7
2.4 漏洞产生原因统计 ..... 8
2.5 漏洞引发威胁统计 ..... 9
2.6 漏洞增长趋势 ..... 10
第三章 CVE 漏洞库安全漏洞概况 ..... 12
3.1 漏洞影响厂商分布情况 ..... 12
3.2 高危漏洞披露时间趋势图 ..... 13
3.3 攻击途径概况 ..... 14
3.4 漏洞影响平台分类 ..... 15
3.5 漏洞类型统计概况 ..... 16
3.6 POC 公开情况统计 ..... 18
第四章 漏洞预警统计情况 ..... 20
4.1 漏洞厂商情况 ..... 20
4.2 漏洞威胁情况 ..... 22
4.3 年度 TOP10 高危漏洞 ..... 23
4.4 漏洞预警 TOP10 漏洞回顾 ..... 25
第五章 总结 ..... 30
5.1 安全防护建议 ..... 30
5.2 漏洞态势展望 ..... 33

# 前言

2022 年在国家出台了新网络安全法规的推动下，网络空间安全日益受到重视。随着政府部门和企业对网络安全的投入增加，网络安全产业也迎来了快速发展的机遇，但与此同时，许多企业和个人受疫情影响更加依赖网络，网络攻击手段的日新月异使得网络空间安全漏洞依然是一个棘手的问题。在国际冲突和疫情的叠加影响下，全球网络空间的对抗升级已经成为不容忽视的现实。随着国家间网络攻击和网络犯罪活动的频繁出现，相应的漏洞利用事件也在不断增加，保护和维护网络安全已成为越来越重要的任务。为了应对这些挑战，必须加强网络安全信息共享和工作协同，强调提升网络安全整体防护能力。同时，随着数字化和云化的普及，安全漏洞成为了保障网络安全的基础。因此，我们必须采取积极的措施，加强网络安全管理和漏洞预警，确保及时修复漏洞，防止漏洞被利用。

作为网络安全领域的领导者，天融信一直致力于推动网络安全技术的发展和应用，并通过不断的探索和实践为客户提供全方位的网络安全服务。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《2022 年网络空间安全漏洞分析研究报告》，在这份报告中，我们将通过实际案例和数据分析，为广大客户和读者提供有价值的信息。

本报告重点内容共分三个部分，第一部分为 2022 年漏洞趋势，通过对 CNVD 漏洞信息库及 CVE 高危漏洞 CVSS 评分 TOP100 漏洞数据进行综合分析而产生。据 CNVD 公开数据显示，2021 年共披露漏洞 26558 枚，2022 年共披露漏洞 23900 枚，同比降低 10%。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 11.13%，中危漏洞占 53.82%，高危漏洞占 35.05%。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 2022 年度高危漏洞预警情况概述,在 2022 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，经过实验室人员快速研判分析，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。2022 年度重点漏洞含 Microsoft Windows 支持诊断工具（MSDT）远程代码执行漏洞、Exchange Server 远程代码执行漏洞、Spring Framework 任意文件写入漏洞、Spring Cloud Gateway 远程代码执行漏洞等。实验室第一时间监测到漏洞后，进行了漏洞复现和应急响应处理，并给出临时缓解方案，保障了客户网络环境安全。

第三部分为 2022 年度总结及展望，天融信阿尔法实验室通过对 CNVD 披露的漏洞数量和 CVE TOP 100 漏洞以及年度预警情况进行了分析总结，并对 2023 年漏洞趋势做出了相关预测。

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，即能够追查攻击来源，查找攻击路径，找出攻击工具，以便有效地防御和应对未来攻击。

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，为国家网络安全进行全方位赋能。

## CNVD漏洞库安全漏洞概况

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 CNVD 漏洞数据库数据,对 2022 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。然而，2022 年的数据显示漏洞数量有所下降。这可能表明，在近一年的时间里，企事业单位和软件开发者采取了有效措施来防止漏洞的产生和利用，从而降低了漏洞的数量。但由于网络安全威胁的持续存在，仍然有必要继续加强网络安全防护。

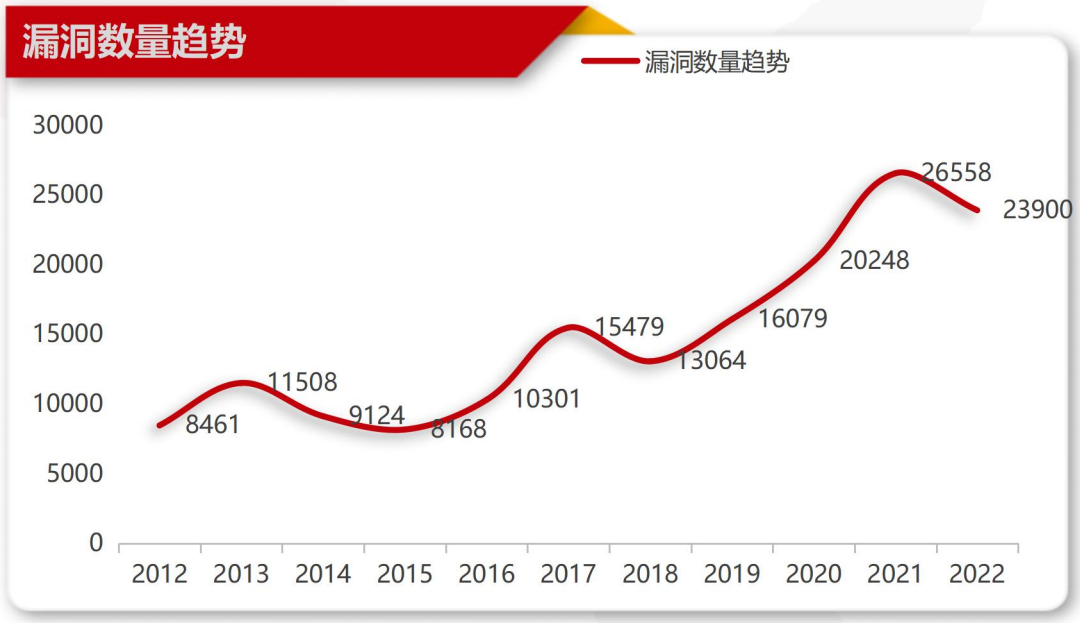


图 1 近十年漏洞数量走势图(数据来自于 CNVD)

### 2.1 漏洞威胁等级统计

根据 2022 年 1-12 月漏洞引发威胁严重程度统计，其中低危漏洞占 11.13%，中危漏洞占 53.82%，高危漏洞占 35.05%。

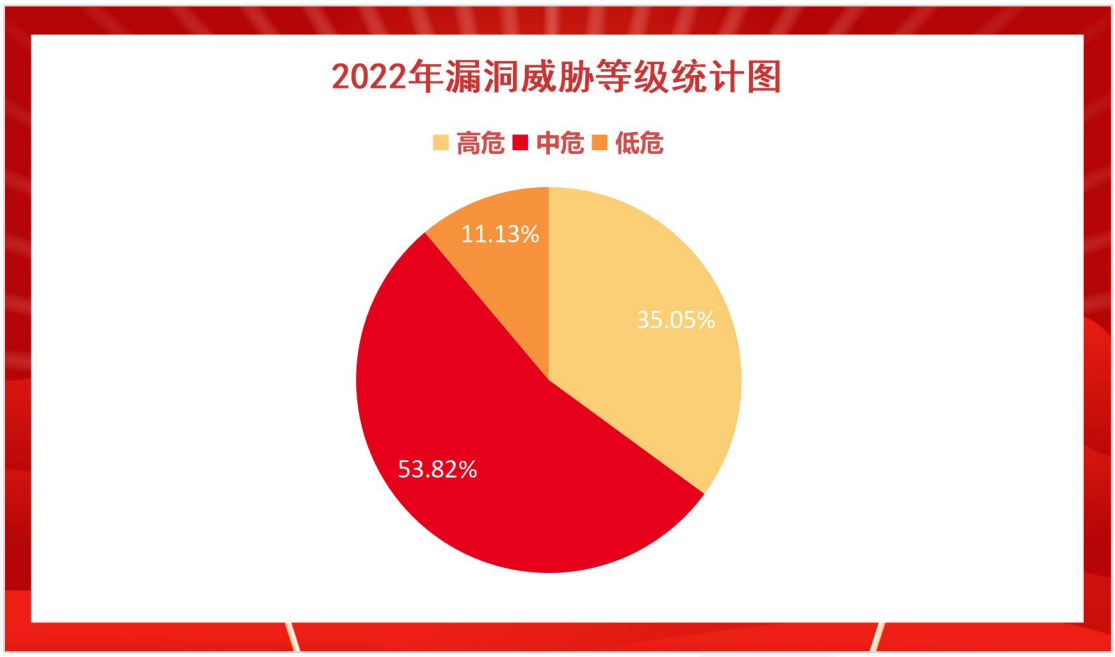


图 2 2022 年收录漏洞按威胁级别统计(数据来自于 CNVD)

可以看出大多数漏洞为中高危。这意味着如果这些漏洞被利用，可能会对网络造成严重的损害。因此，企业组织需要重视漏洞管理工作，并加强对中高危漏洞的修补和防护。同时，这也提醒企业组织需要注意资产的安全性，虽然低危漏洞只有 11.13% ，但如果这些资产很重要或者被大量使用，仍然有可能带来潜在的风险。

## 2.2 漏洞利用攻击位置统计

根据 2022 年 1-12 月漏洞利用攻击位置统计，其中远程攻击占比约为 82.5%，本地攻击约占 13.5%，其他攻击为 4.0%。

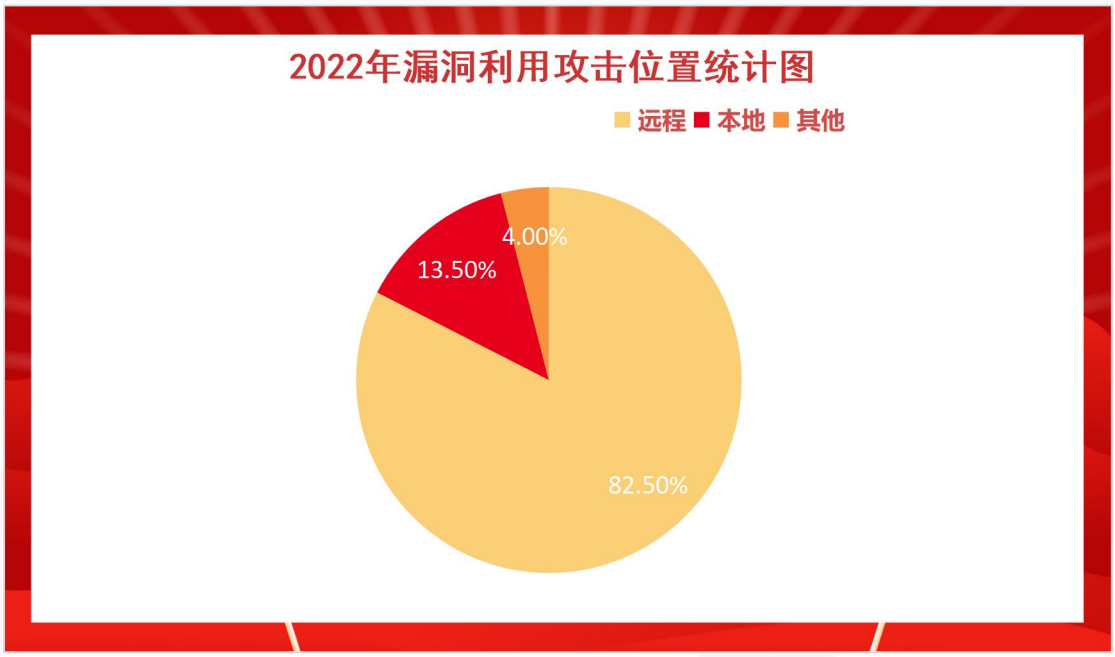


图 3 2022 年收录漏洞利用的攻击位置统计（数据来自于 CNVD）

由此可见，远程攻击是主要的漏洞攻击手段，且更具有潜在危险。因此，对企业组织来说，保护外部接入点更加重要，安全团队应加强对网络边界的审查和保护。此外，尽管本地攻击和其他类型的攻击所占比例较小，但这并不意味着可以忽略这部分攻击的风险，仍然是一种需要警惕的攻击方式。其他类型的攻击可能包括例如物联网设备、工业控制系统等非传统网络设备的攻击，这些设备可能不具备足够的安全防护措施，因此需要加强对这些设备的安全监控和保护。

## 2.3 漏洞影响对象类型统计

根据 2022 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、数据库、安全产品、工业控制系统。其中 WEB 应用漏洞 43.8%，应用程序漏洞 28.7%，网络设备漏洞 13.9%，操作系统漏洞 4.8%，智能设备漏洞 4.5%，数据库漏洞 1.6%，安全产品漏洞 1.5%，工业控制系统漏洞 1.3%。

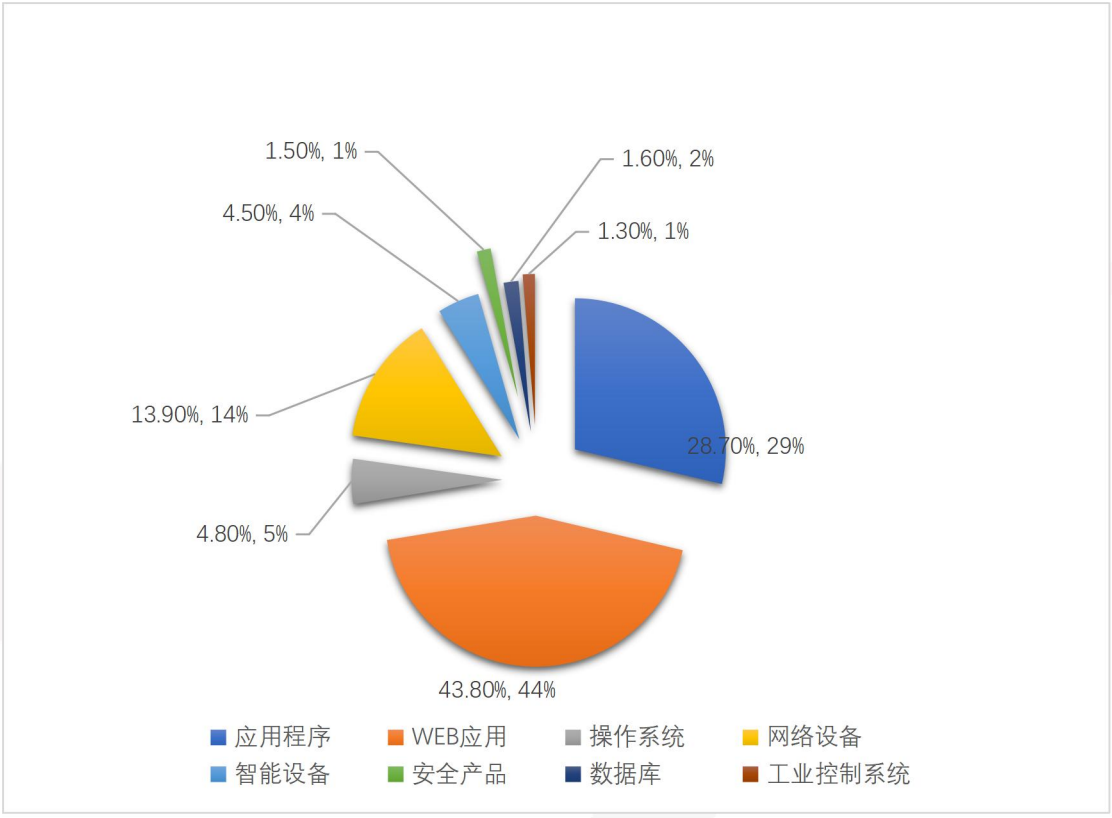


图 4 2022 年漏洞影响对象类型统计(数据来自于 CNVD)

由此可见，应用程序漏洞和 WEB 应用漏洞是导致威胁的主要原因，占据了总数的 72.5%。天融信提供政府、金融、交通、运营商、教育、卫生等行业安全场景解决方案，可以有效解决此类应用程序在实际场景中存在的各类安全问题。企业组织在进行渗透测试或代码审计时，也应首先关注这两类产品可能出现的大量漏洞。虽然操作系统漏洞所占比例较小，但由于操作系统是整个网络的基础，因此也应加强对操作系统的安全防护。此外，尽管智能设备漏洞、安全产品漏洞和数据库漏洞所占比例较小，但也应加强对这些方面的安全性评估。特别是在工业控制系统方面，由于其对社会基础设施起关键性作用，应特别重视工业控制系统的安全防护。

## 2.4 漏洞产生原因统计

根据 2022 年 1-12 月漏洞产生原因的统计，设计错误导致的漏洞占比 68.1% ，屈居首位，紧跟其后的是输入验证错误导致的漏洞占比 27.4%，位居第二，接着是边界条件错误导致的漏洞占比 3.1%，位居第三。后面的访问验证错误、竞争错误、其他错误、配置错误、环境错误、意外情况处理错误分别占比 1.1%、 0.2%、0.1%、0.01%、0.004%、0.004%。

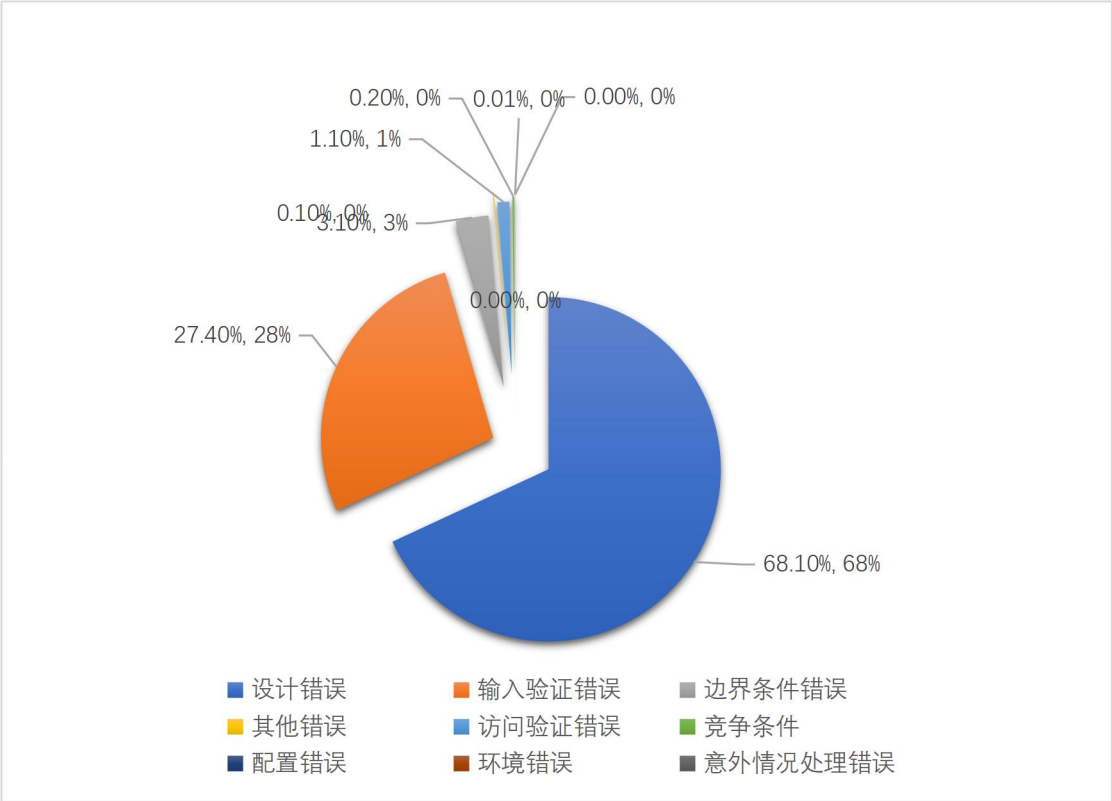


图 5 2022 年漏洞产生原因统计(数据来自于 CNVD)

由此可见，设计错误是导致漏洞的主要原因。这说明系统在项目设计之初，可能并未全面地考虑自身的安全性需求，导致系统存在漏洞。这种漏洞可能难以在输入输出测试中发现，因此在设计系统时应使用安全设计原则确保系统的安全性。此外，输入验证错误也是一个常见的导致漏洞原因，输入验证是指对于外部输入的数据进行校验的过程。这是一种重要的安全措施，因为在许多情况下，恶意用户会尝试向系统注入恶意数据，以便破坏系统或获取敏感信息。软件开发人员往往忽略了对输入数据进行足够的校验。这种漏洞通常危害大，因为它们可能允许攻击者执行任意代码或获取敏感信息。同时，这种漏洞通常很容易利用，因为攻击者可以使用自动化工具来构造恶意输入并测试系统的输入验证。为了避免输入验证错误，软件开发人员应该加强对输入数据的验证，包括对数据类型、格式和范围的检查。例如，如果系统期望接收用户年龄的输入，则应该确保输入的数据是整数，并且在合理范围内。这样可以避免恶意用户输入字符串或超出范围的数字，从而导致系统异常。尽管其他原因所占比例较小，但仍然应加强对系统的访问验证、竞争、配置和环境的安全性评估，以确保系统的安全性。

## 2.5 漏洞引发威胁统计

根据 2022 年 1-12 月漏洞引发威胁统计，未授权的信息泄露占比 45.5%居首位，管理员访问权限获取占比 27.6%位居第二，拒绝服务占比 14.0%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、未知。占比分别是 12.1%、0.5%、0.3%、0.1%。

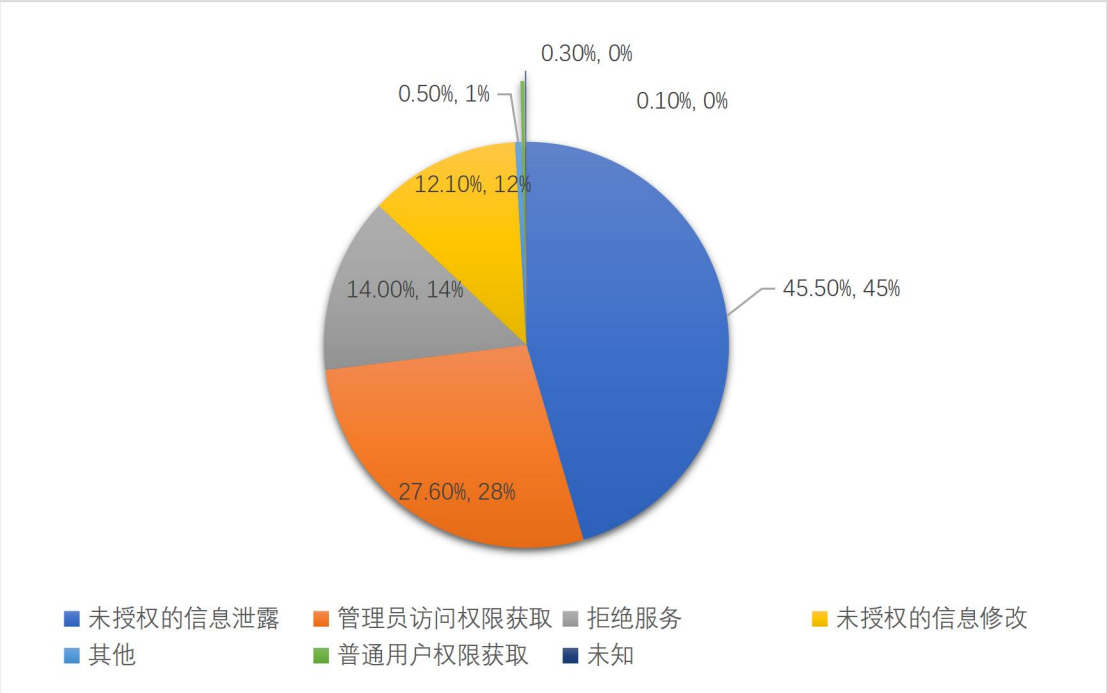


图 6 2022 年漏洞引发威胁统计(数据来自于 CNVD)

由此可见，未授权的信息泄露是导致威胁的主要原因，数据即生命，数据泄露可能会对企业造成无法估量的损失，保护信息安全是非常重要的。因此，有效的数据防泄漏系统是必不可少的。天融信网络数据防泄漏系统通过深度的内容识别、敏锐的行为感知、多样化的部署方式、全覆盖业务系统应用场景、全面的流动监控、迅速的泄漏响应、开放的架构设计、灵活的交付部署来帮助企业保护数据安全。同时，管理员访问权限获取也是值得关注的重点，在保护网络安全时，应加强对管理员访问权限的保护，避免使用弱口令等导致攻击者恶意获取管理员权限。此外，拒绝服务也是一种威胁。拒绝服务攻击可以通过多种方式实现，包括但不限于：利用脚本模拟大量用户请求、使用僵尸网络发起攻击、利用漏洞导致服务器资源耗尽等。如果未得到及时有效的防护，拒绝服务攻击可能会对信息系统和业务造成严重的影响，包括网站瘫痪、服务中断、数据丢失、用户流失等。因此，加强对系统服务的保护是非常重要的，应使用多种方法来防护拒绝服务攻击，包括但不限于：安装防火墙、使用 DDOS 防护设备、进行服务器优化和加固等。最后，也应注意未授权的信息获取、普通用户权限获取等方面的威胁，加强相应的安全防护。

## 2.6 漏洞增长趋势

通过 CNVD 漏洞信息库对 2021、2022 漏洞公开数据显示，2021 年一共披露漏洞 26558 枚，2022 年一共披露漏洞 23900 枚。同比减少 10%，2021 年高危漏洞 7284，2022 年高危

漏洞 8379 枚，同比 2021 年增加 15.03%，2021 年中危漏洞 15738 枚，2022 年中危漏洞 12862 枚，同比 2021 年减少 18.27%，2021 年低危漏洞 3536 枚，2022 年低危漏洞 2659 枚，同比 2021 年减少 16.32%。

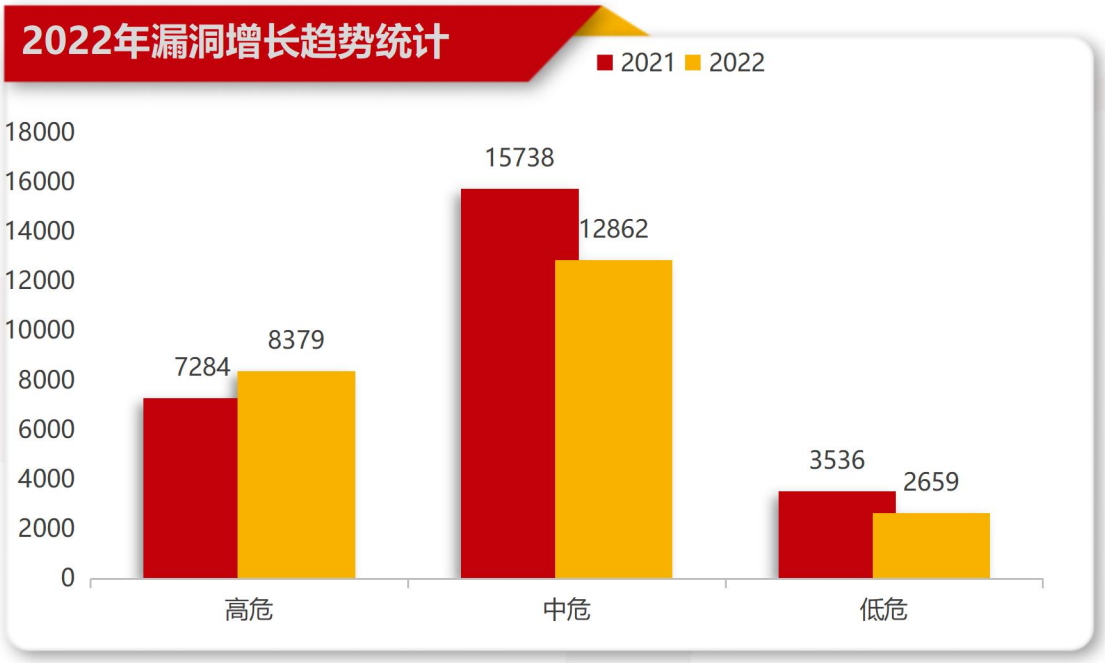


图 7 2022 年漏洞增长趋势统计（数据来自 CNVD）

根据这份数据我们可以看出，2022 年的漏洞总数相较于 2021 年有所减少，这可能是因为企业和机构在过去一年里加强了对漏洞的检测和修复或者因为在软件开发过程中更加注重了安全性。然而，从高危漏洞的数量来看，2022 年的数量略微高于 2021 年，这说明有些高危漏洞并没有得到很好的修复，存在潜在的威胁。为了提高漏洞管理效率，需要不断优化漏洞管理计划的成熟度和有效性，加强漏洞管理流程。此外，还需注意不同级别漏洞的处理优先级，高风险和严重风险漏洞需要尽快修复，但也不要忽略低风险和中等风险漏洞的修复。同时也要尽力在预算允许的范围内招募和培养安全人才，并定期评估和更新漏洞管理规程，从而更有效地保护自己的网络安全。

# CVE漏洞库安全漏洞概况

通过对 CVE 在 2022 年公布的漏洞按 CVSS 评分高低进行排序,我们筛选了 CVSS 基本评分最高的前 100 个漏洞进行统计分析。此次统计分析主要从漏洞所影响厂商、影响平台、攻击途径、披露时间、漏洞类型以及 POC 公开情况等 6 个方面展开。结果显示，漏洞影响厂商前三名分别是谷歌、台达及思科。从影响的平台进行统计，受影响的平台大致可分为五类:分别是 PC 端平台、移动端平台、硬件设备平台、跨平台以及其他平台。其中硬件设备平台 38%，占据首位。由此可见漏洞依然集中在传统厂商的设备和产品中，且主流系统和产品所面临的漏洞威胁和安全风险较大。

而从高危漏洞的披露时间看，2 月份共披露高危漏洞 22 个，位居全年第一。在 TOP100 漏洞中大约有 17%的高危漏洞存在公开 POC，这一数据占比相比往年提高。公开 POC 可能会为攻击者提供便利条件，使其能够更快地研发攻击工具，这将对相关软硬件设备造成重大安全威胁，并给用户带来威胁。为了避免这种情况的发生，开发者应该在软件设计和开发阶段就考虑安全问题，并采取有效措施来防范漏洞的产生。

从攻击途径看可被远程利用的漏洞占比约为 98%，本地利用的漏洞约占 2%，这表明大多数漏洞都是可以被远程利用的，只有很少一部分漏洞可以被本地利用。因此，为了保证网络安全，我们应该采取更多有效措施，防止远程攻击。从披露漏洞危害程度前 100 例的统计数据可以看出，远程代码执行漏洞、SQL 注入漏洞、命令注入漏洞是当前网络安全形势下最为严峻的威胁，它们共同占比超过 50%。未来，我们应该加强网络安全管理，健全安全技术，针对这些漏洞提供有效的防护措施，以期确保网络安全。具体统计分析结果如下:

## 3.1 漏洞影响厂商分布情况

根据 2022 年 1-12 月 CVE 披露漏洞危害程度前 100 例所影响的相同厂商情况进行统计，前三名分别是谷歌、台达及思科。其中谷歌厂商的产品占比达到 17.00%，台达的产品占到 11.00%，思科的产品共占 5.00%。

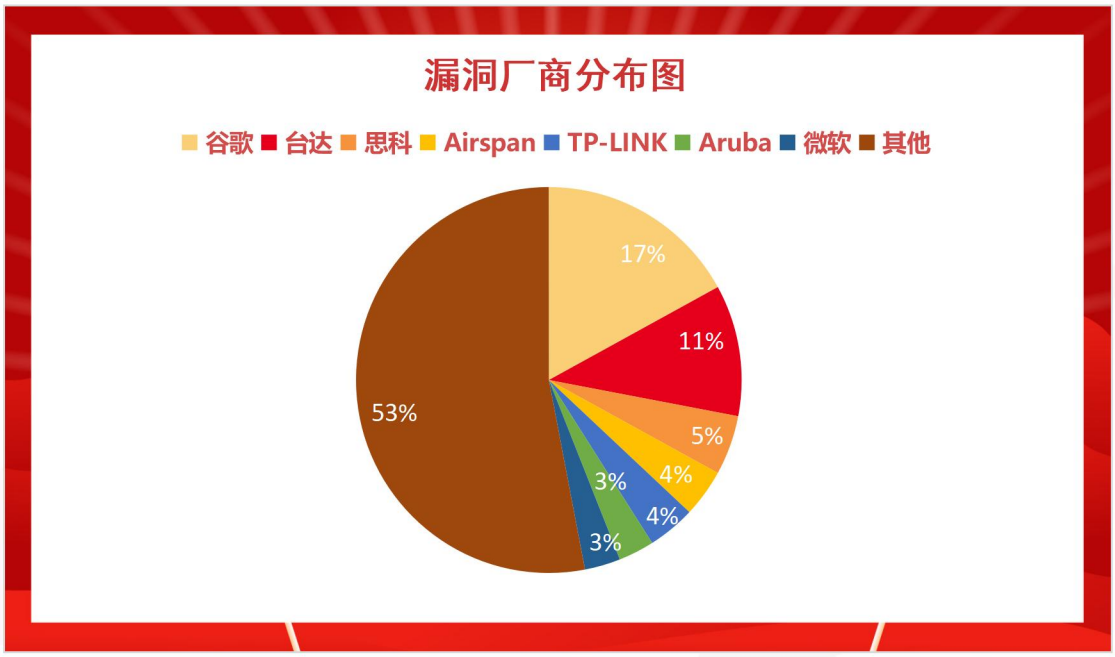


图 8 漏洞厂商分布图(数据来自于 CVE)

谷歌、台达和思科是在 2022 年 1-12 月中受到漏洞攻击最多的厂商。这也意味着，如果你正在使用谷歌、台达或思科的产品，就应该特别注意保护这些产品的安全。可以考虑采取一些措施来防范漏洞的利用，例如定期更新其应用程序的安全补丁，使用相应的安全产品来监测网络流量，并在发现异常时立即采取行动。定期对网络进行安全审计，以找出并修复潜在的漏洞。最后，还要注意不要下载来自不信任来源的文件，也不要点击未知的链接，以避免意外地触发漏洞。通过这些措施，可以有效地降低遭受漏洞攻击的风险。

## 3.2 高危漏洞披露时间趋势图

根据 2022 年 1-12 月 CVE 披露漏洞危害程度前 100 例相同披露时间进行统计，在 2022 年全年中，2 月份披露 22 个，占比 22%位居第一，6 月份披露 21 个，占比 21%位居第二，5 月份披露 20 个，占比 20%位居第三。

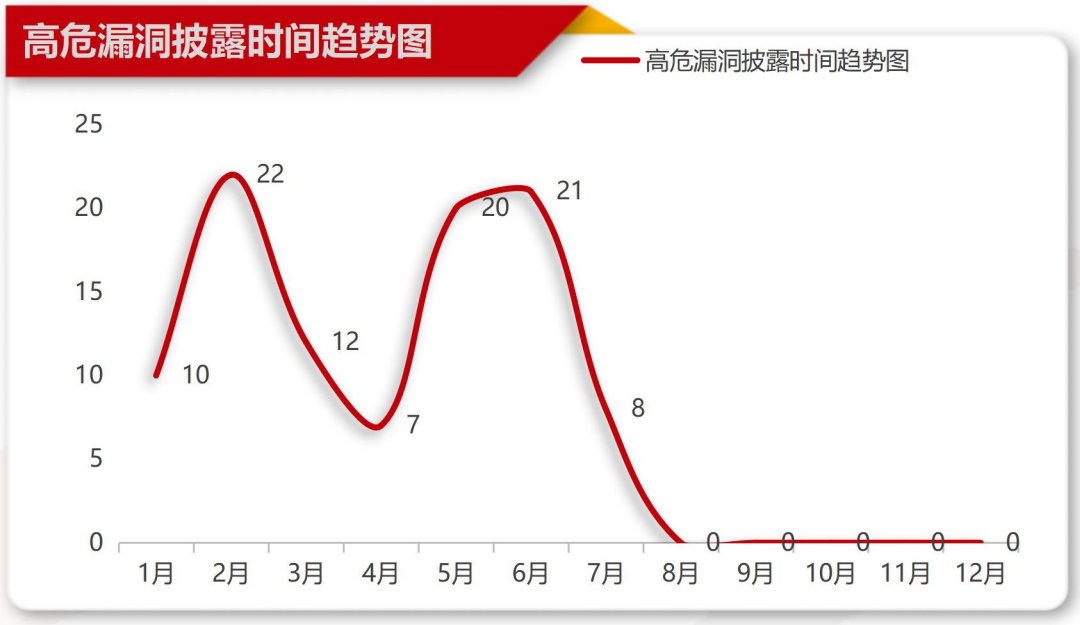


图 9 高危漏洞披露时间趋势图(数据来自于 CVE)

## 3.3 攻击途径概况

根据 2022 年 1-12 月 CVE 披露漏洞危害程度前 100 例相同攻击途径进行统计，其中来自远程攻击占比约为 98%，本地攻击约占 2%。

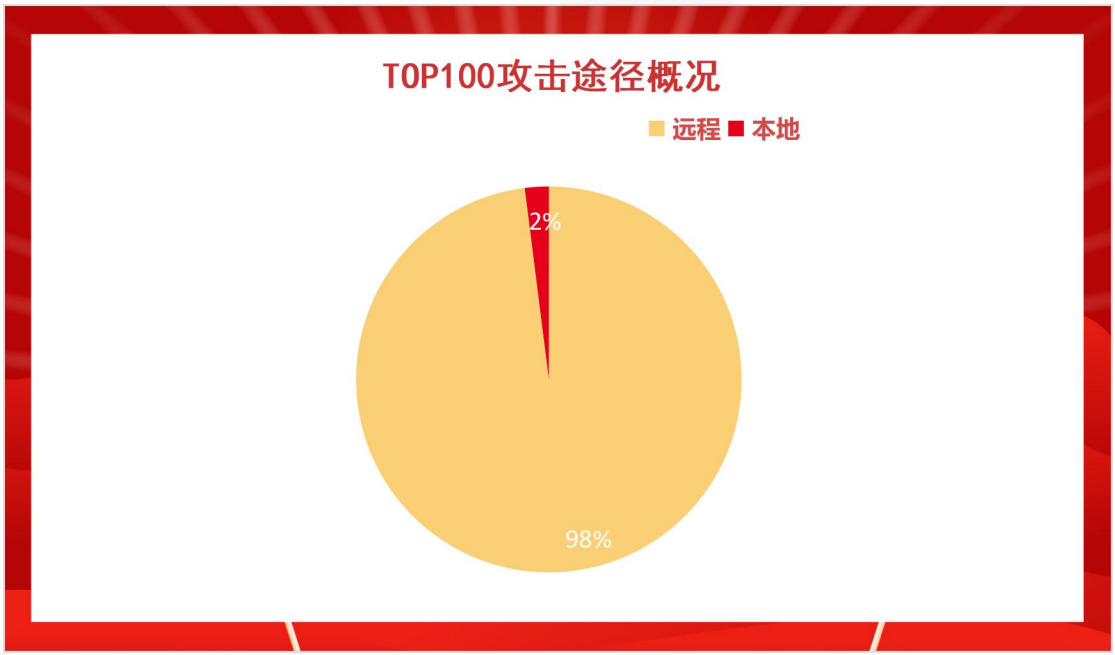


图 10 TOP100 攻击途径概况(数据来自于 CVE)

2022 年远程攻击漏洞数量占比提升。这表明，远程攻击是当前攻击者采用的主要攻击手段，要有效防范网络攻击，应该优先考虑和加强安全策略的实施、进行综合性的安全防御、严格控制网络访问权限、定期进行安全漏洞扫描、保护网络的关键资源、以及采用多层防护技术，这些措施都可以有效地防止远程攻击。

## 3.4 漏洞影响平台分类

根据 2022 年 1-12 月 CVE 披露漏洞危害程度前 100 例所影响的平台进行统计，受影响的平台大致可分为五类:分别是硬件设备平台、PC 端平台、跨平台、移动端平台以及其他平台。其中硬件设备平台 38%、PC 端平台 19%、跨平台 18%、移动端平台 15%、其他平台 10%。

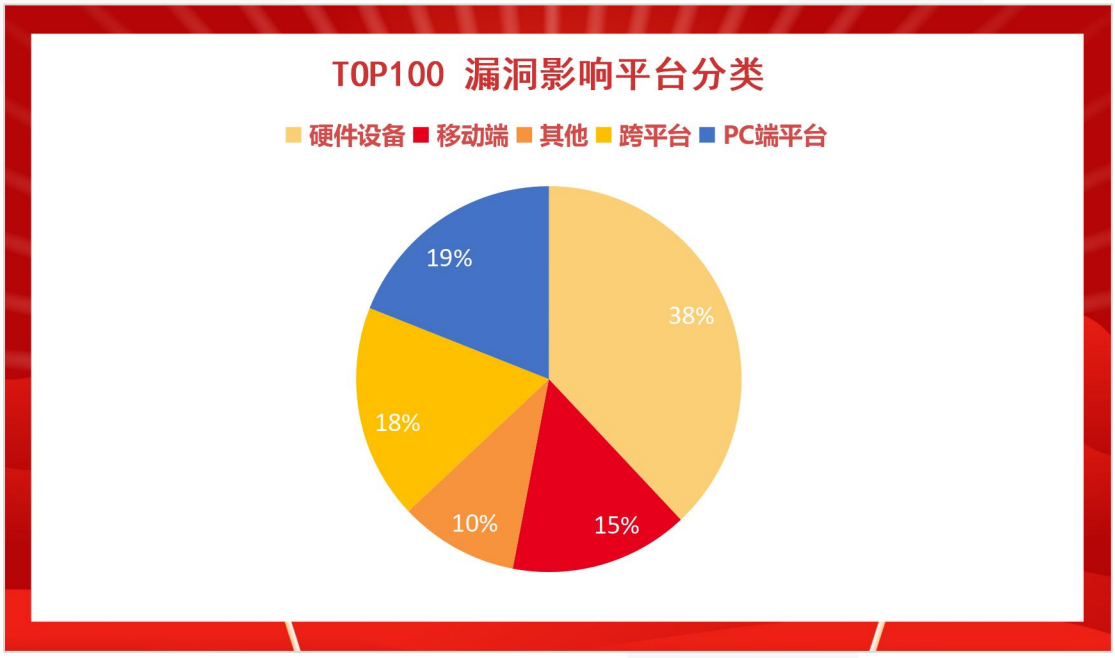


图 11 TOP100 漏洞平台分类(数据来自于 CVE)

这些数据表明，硬件设备平台受到的漏洞攻击最多，由于硬件设备的复杂度较高，其更新迭代速度较慢，导致在设计、开发和使用过程中容易出现漏洞。另外，PC 端平台和跨平台也受到了较多的漏洞攻击，这与 PC 端平台和跨平台的广泛使用密切相关。而移动端平台的漏洞攻击相对较少，移动端平台的安全机制相对比较完善，更新迭代速度较快，使得漏洞得到及时修复。总的来看，各类平台都需要加强对漏洞的防范和修复工作，以确保系统和设备的安全。

## 3.5 漏洞类型统计概况

根据 2022 年 1-12 月 CVE 披露漏洞危害程度前 100 例相同类型进行统计，其中远程代码执行漏洞占比最多，以 28%位居首位，而 SQL 注入占比 15%、命令注入占比 11%、权限提升占比 8%、访问控制不当 6%、越界写入占比 5%、身份验证绕过占比 4%、其他漏洞占比 15%。

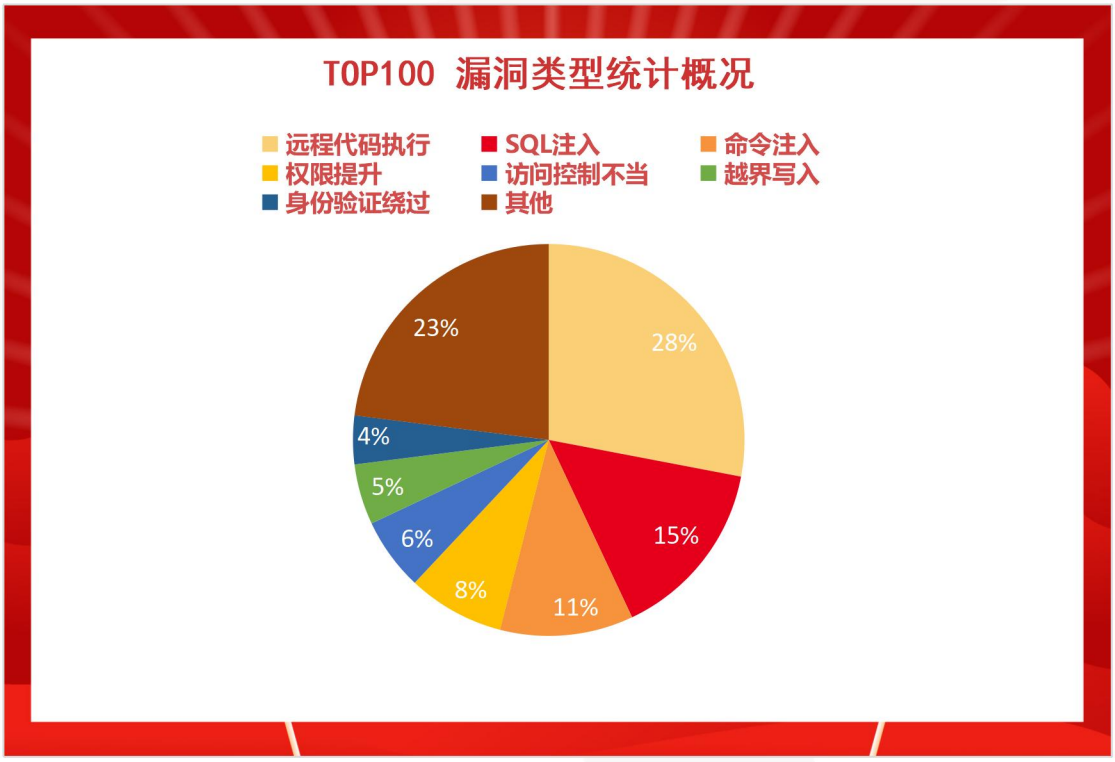


图 12 TOP100 漏洞类型统计概况(数据来自于 CVE)

远程代码执行漏洞是最常见的漏洞类型，其次是 SQL 注入和命令注入。可以考虑采用一些措施来防范漏洞的利用，例如使用输入验证、边界检查和访问控制等技术来防止攻击者利用漏洞进行攻击。此外，定期更新操作系统和应用程序的安全补丁也是很有必要的，这可以帮助系统修复已知的漏洞，防止攻击者利用这些漏洞进行攻击。

根据 MITRE 今年通过对公开可用的国家漏洞数据库中 37000 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 2021 年排名相比 |
|---|---|---|---|---|
| 1 | CWE-787 | 越界写入 | 64.20 | 0 |
| 2 | CWE-79 | 跨站脚本 | 45.97 | 0 |
| 3 | CWE-89 | SQL 注入 | 22.11 | +3 |
| 4 | CWE-20 | 输入验证不当 | 20.63 | 0 |

| | | | | |
|---|---|---|---|---|
| | CWE-125 | 越界读取 | 17.67 | -2 |
| 6 | CWE-78 | OS 命令注入 | 17.53 | -1 |
| 7 | CWE-416 | Use-After-Free | 15.50 | 0 |
| 8 | CWE-22 | 路径遍历 | 14.08 | 0 |
| 9 | CWE-352 | 跨站请求伪造 (CSRF) | 11.53 | 0 |
| 10 | CWE-434 | 文件上传 | 9.56 | 0 |
| 11 | CWE-476 | NULL 指针解引用 | 7.15 | +4 |
| 12 | CWE-502 | 反序列化 | 6.68 | +1 |
| 13 | CWE-190 | 整数溢出 | 6.53 | -1 |
| 14 | CWE-287 | 身份验证不当 | 6.35 | 0 |
| 15 | CWE-798 | 使用硬编码凭证 | 5.66 | +1 |
| 16 | CWE-862 | 缺少授权 | 5.53 | +2 |
| 17 | CWE-77 | 命令注入 | 5.42 | +8 |
| 18 | CWE-306 | 缺少关键功能的身份验证 | 5.15 | -7 |
| 19 | CWE-119 | 内存缓冲区范围内的操作限制不当 | 4.85 | -2 |
| 20 | CWE-276 | 不正确的默认权限 | 4.84 | -1 |
| 21 | CWE-918 | 服务器端请求伪造 (SSRF) | 4.27 | +3 |
| 22 | CWE-362 | 竞争条件 | 3.57 | +11 |
| 23 | CWE-400 | 不受控制的资源消耗 | 3.56 | +4 |
| 24 | CWE-611 | XML 外部实体引用限制不当 | 3.38 | -1 |
| 25 | CWE-94 | 代码注入 | 3.32 | +3 |

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更具体的基础层漏洞，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-362（竞争条件）：从第 33 名提升到第 22 名；

（2） CWE-94（代码注入）：从第 28 名提升到第 25 名；

（3） CWE-400（不受控制的资源消耗）：从第 27 名提升到第 23 名；

（4） CWE-77（命令注入）：从第 25 名提升到第 17 名；

（5） CWE-476（NULL 指针解引用）：从第 15 名提升到第 11 名。

**排名大幅下降的漏洞有：**

（1） CWE-306（缺少关键功能的身份验证）：从第 11 名下降到第 18 名；

（2） CWE-200（未授权访问敏感信息）：从第 20 名下降到第 33 名；

（3） CWE-522（凭证失效）：从第 21 名下降到第 38 名；

（4） CWE-732（权限分配错误）：从第 22 名下降到第 30 名。

**Top 25 中的新入围的漏洞有：**

（1） CWE-362（竞争条件）：从第 33 名上升到第 22 名；

（2） CWE-94（代码注入）：从第 28 名上升到第 25 名；

（3） CWE-400（不受控制的资源消耗）：从第 27 名上升到第 23 名。

**从 Top 25 中落选的漏洞有：**

（1） CWE-200（未授权访问敏感信息）：从第 20 名降至第 33 名；

（2） CWE-522（凭据失效）：从第 21 名降至第 38 名；

（3） CWE-732（权限分配错误）：从第 22 名降至第 30 名。

## 3.6 POC 公开情况统计

根据 2022 年 1-12 月 CVE 披露漏洞危害程度前 100 例 POC 公开情况进行统计，其中未公开 POC 居多，占比 83%，公开 POC 的仅有 17%。

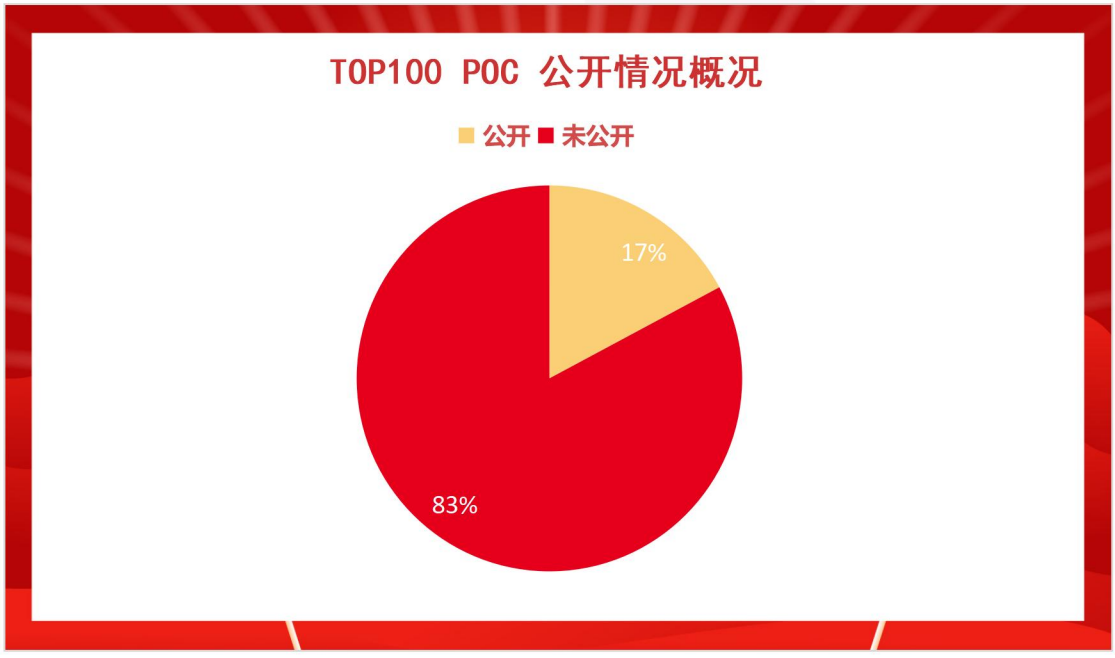

图 13 TOP100POC 公开情况概况(数据来自于 CVE)

由此可见，大多数漏洞没有被正确有效地揭示出来。及时更新软件修复版本可以有效地防止漏洞利用的产生。企业可以采用自动化补丁管理流程，通过使用自动化工具来监控补丁发布，并自动部署补丁，来提高应用补丁的速度和效率。这样做还能帮助企业避免人为错误，并减少补丁管理过程中的工作量。在快速应用安全补丁的同时，也需要确保补丁的有效性。补丁应用过程中，应该进行测试，以确保补丁不会对系统性能造成负面影响。同时也应该对补丁进行监控，以确保补丁能够有效修复漏洞。此外企业安全团队需要准确的漏洞信息，仅依靠公开的漏洞库可能不够充分，因此有必要引入并收集更多的漏洞资源。拥有更充分的漏洞信息可以帮助安全团队更准确地评估漏洞的可利用性和是否存在解决方案，从而更有针对性地进行漏洞修复。

# 漏洞预警统计情况

2022 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 45627 条，经过漏洞监测系统自动智能筛选后留存高危漏洞信息 365 条，进一步经人工研判后发布高危漏洞风险提示通告 62 条。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。2022 年针对 Microsoft 厂商漏洞预警次数达 15 次，其中 Windows 系统的漏洞占大多数。OpenSSL、Vmware 等关键基础设施漏洞也是受关注度较高的方向。

2022 年预警的漏洞中，代码执行类漏洞占比最高，达到 71%。这一类漏洞也是 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即可达到远程代码执行的效果，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 2022 年内发布的 62 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 15 次，占比约 24%，针对 Google 和 Apache 的均为 6 次，占比 10%，并列第二名。

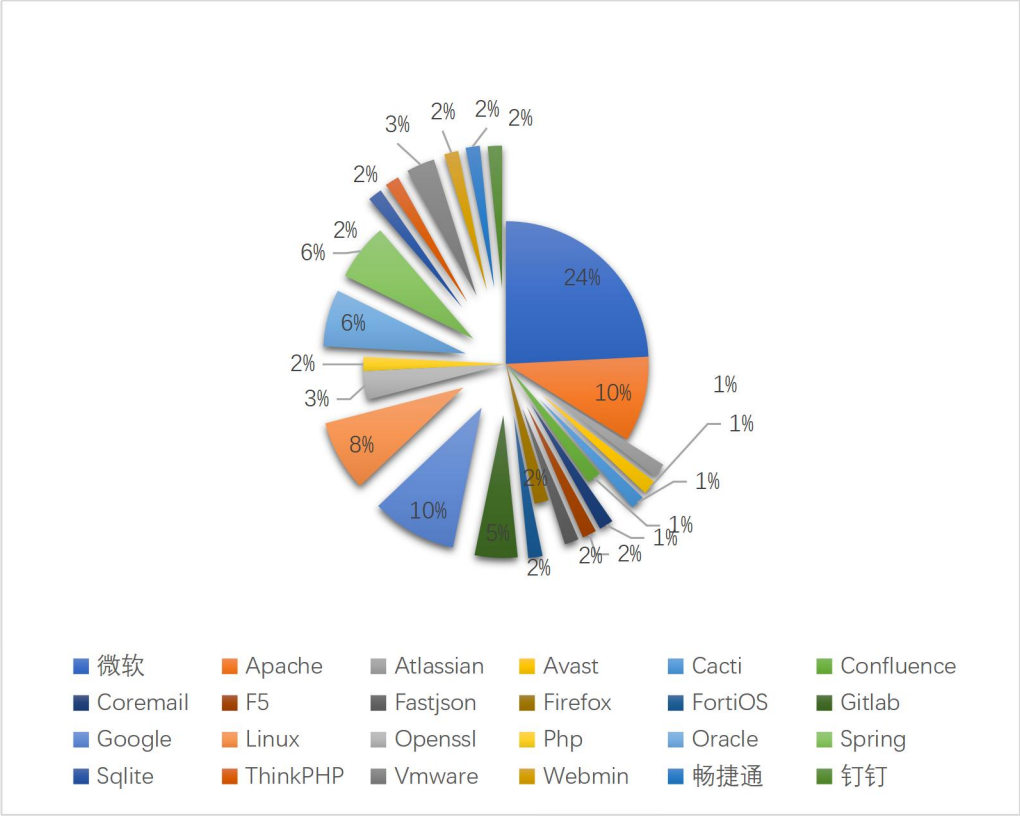


图 14 2022 年漏洞预警厂商情况

从整体情况来看，微软使用广泛、影响力大无疑是一个重要因素，同时其也非常重视安全性，一直依靠强大的安全能力来应对各种外部攻击。由于微软的产品影响力如此之大，因此涉及到的安全风险也就更大。就算是在合理或者正常的使用情况下，也有可能出现未修补的危险问题。因此，在使用微软产品的过程中，应当特别注意安全问题，及时更新修复版本，防止漏洞被利用。同时，对于使用微软产品的组织或者个人来说，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。

Google 在技术开源方面做出了巨大贡献。其广泛发布使用的开源代码应用，为业界带来了许多方便。然而，由于 Google 产品涵盖面广，涉及的行业和领域也各不相同，因此其所面临的风险也各有不同。包含浏览器、智能手机、云计算、物联网、大数据存储、移动应用程序、自动驾驶等领域。例如，在浏览器领域，Google Chrome 可能会面临 V8 引擎内核漏洞、浏览器扩展漏洞、第三方应用漏洞以及针对浏览器恶意软件的威胁。个别风险来源于其使用的开源组件，因此需要密切关注漏洞修复情况并及时升级。此外，用户也应该注意自己的网络安全，避免下载未知来源的软件以及注意保护个人信息。在智能手机市场，开源的 Android 系统底层代码对所有人都是可见的，这意味着任何人都可以检查代码，寻找潜在的漏洞并尝试利用它们。因此，Android 系统也会面临着来自第三方应用或恶意软件利用系统漏洞的威胁，这些漏洞可能会被黑客用来获取用户的个人信息或者控制用户的设备。此外，由于 Android 市场份额的巨大优势，它也可能成为攻击者针对的主要目标。

为了应对这些威胁，Android 开发商必须不断加强系统安全性，并且需要不断地对系统进行更新以修补漏洞。Android 用户也应该注意安装来自可靠来源的应用，并且应该及时安装系统更新以保证信息安全。

在 Web 架构中，开源软件的应用范围同样广泛，不仅如 Log4j 这样的日志组件会受到攻击者的影响，还有像 Tomcat、Dubbo、Solr、Hadoop 等 Apache 软件基金会管理的顶级开源项目也都存在被攻击的可能性。由于组件之间存在相互依赖关系，一旦存在安全漏洞，就会导致漏洞在组件之间传播，从而影响到 90%以上基于 Java 开发的应用平台。因此，我们在使用开源软件时，一定要制订完善的安全管理措施，以防止开源软件带来的漏洞威胁。

## 4.2 漏洞威胁情况

在 2022 年发布的 62 条漏洞通告中，所通告的漏洞可分为 8 大类，分别是远程代码执行漏洞、权限提升漏洞、身份验证绕过漏洞、任意文件上传漏洞、拒绝服务漏洞、命令注入漏洞、沙箱逃逸漏洞，其中代码执行漏洞占比 71%，位于首位，权限提升漏洞占比 10%，位于第二位，身份验证绕过漏洞占比 8%，位于第三位。

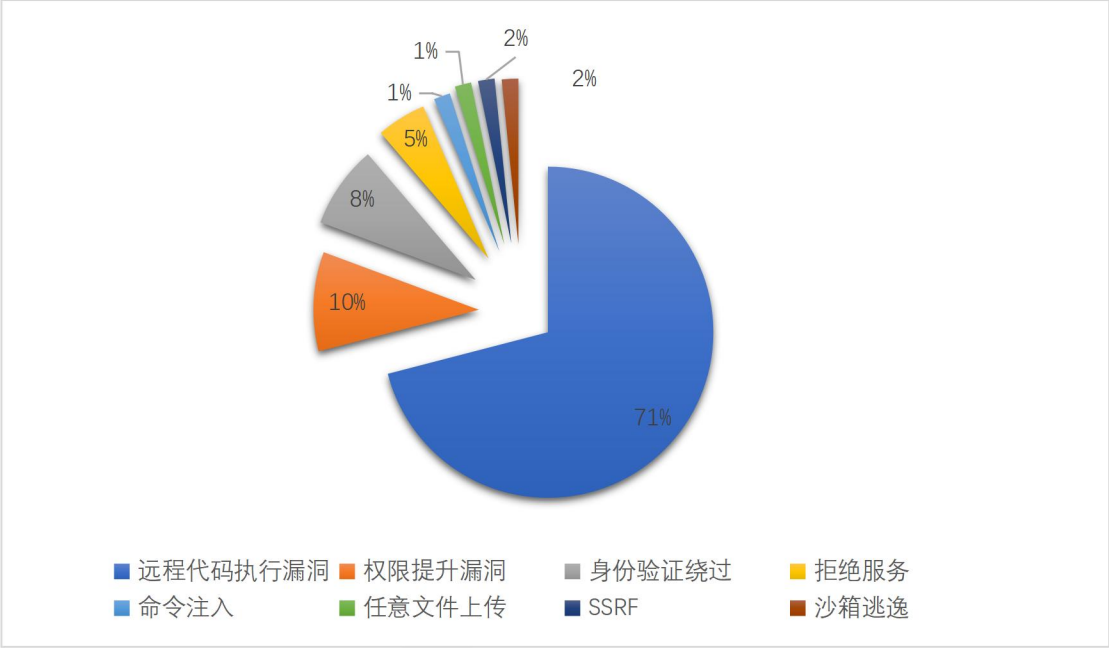


图 15 2022 年预警漏洞威胁情况

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，这类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。紧随其后的是身份验证绕过漏洞，这类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。在其他漏洞类型中，任意文件上传漏洞、拒绝服务漏洞、命令注入漏洞和沙箱逃逸

漏洞的比例都较低，但仍需引起重视。任意文件上传漏洞可能导致未经授权的文件被上传到系统中，拒绝服务漏洞可能导致系统无法正常运行，命令注入漏洞可能允许攻击者在系统中执行任意命令，而沙箱逃逸漏洞则可以让攻击者跳出限制性安全措施的限制，获取未授权的访问权限。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 2022 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-2022-30190 | Microsoft Windows 支持诊断工具(MSDT) 远程代码执行漏洞 | CVE-2022-30190：远程代码执行漏洞，攻击者可通过恶意 Office 文件中远程模板功能从服务器获取恶意 HTML 文件，通过‘ms-msdt’URI 来执行恶意 PowerShell 代码。该漏洞在宏被禁用的情况下，仍能通过 MSDT（Microsoft Support Diagnostics Tool）功能执行代码，将恶意 doc 文件另存为 RTF 格式时，无需打开文件，通过资源管理器中的预览选项卡即可在目标机器上执行任意代码。 |
| NO.2 | CVE-2022-41082 | Microsoft Exchange Server 远程代码执行漏洞 | CVE-2022-41082：是一个远程命令执行漏洞，要成功利用该漏洞必须先经过身份认证，之后即可利用一个网络调用来触发恶意程序代码。被微软列为重大（Critical）漏洞，经微软证实，黑客们利用 ProxyNotShell 漏洞，在被攻击的 Exchange 服务器上部署了 China Chopper web shell 恶意脚本。这个漏洞在微软发布的 11 月周二补丁包中都已得到了解决。 |
| NO.3 | CVE-2022-22965 | SpringFramework 任意文件写入漏洞 | CVE-2022-22965：该漏洞是 SpringFramework 的一个漏洞，攻击者可以在未授权的情况下，通过发送数据包，在目标服务器上写入任意文件，例如通过漏洞将 WebShell 写入目标服务器，然后通过访问 WebShell 来执行命令，进而获取整个服务器的权限。虽然该漏洞的利用 |

| | | | |
|---|---|---|---|
| | | | 方式并没有那么容易，但是该漏洞已经成为不法犯罪分子的武器，所以值得被关注。 |
| NO.4 | CVE-2022-3723 | Google Chrome 远程代码执行漏洞 | 2022 年 10 月 27 日 google 官方紧急发布 Google Chrome 远程代码执行漏洞 CVE-2022-3723。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。 |
| NO.5 | CVE-2022-1388 | F5 BIG-IP iControl REST 身份验证绕过漏洞 | CVE-2022-1388 该漏洞是一个身份验证绕过漏洞，未经身份验证的攻击者利用此漏洞可以通过管理端口或利用自身 IP 对 BIG-IP 系统进行网络访问绕过身份验证，并且可以任意执行系统命令、创建或删除文件以及禁用 BIG-IP 上的服务。 |
| NO.6 | CVE-2022-25845 | Fastjson 反序列化漏洞 | 此次漏洞的影响范围是≤1.2.80，Fastjson 使用黑白名单用于防御反序列化漏洞,在特定条件下可绕过默认 autoType 关闭限制，攻击远程服务器，风险影响较大。 |
| NO.7 | CVE-2022-22947 | Spring Cloud Gateway 远程代码执行漏洞 | 当启用和暴露不安全的 Gateway Actuator 端点时，使用 Spring Cloud Gateway 的应用程序容易受到代码注入攻击。远程攻击者可以发出恶意制作的请求，成功利用该漏洞可以导致代码执行。 |
| NO.8 | CVE-2021-4034 | Polkit 权限提升漏洞 | CVE-2021-4034 是由于 pkexec 无法正确处理调用参数，从而将环境变量作为命令执行，具有任意用户权限的攻击者都可以在默认配置下通过修改环境变量来利用此漏洞，从而获得受影响主机的 root 权限，漏洞的影响范围较广，应值得被关注。 |
| NO.9 | CVE-2021-31805 | Apache Struts2 远程代码执行 | 导致该漏洞的原因是对 S2-061 修复不够完整，当开发人员使用%{……}语法强制 OGNL 解析时，还是会有一些特殊的标签属性会被二次解析，攻击者可以向受害主机发送恶意的 OGNL 表达式执行任意代码。 |
| NO.10 | CVE-2022-26134 | Atlassian Confluence RCE 漏洞 | 该漏洞允许在未经身份验证的情况下，通过发送恶意的 Web 请求注入命令，实现在受影响的 Confluence Server 或 Data Center 实例上执行任意代码。 |

## 4.4 漏洞预警 TOP10 漏洞回顾

### 4.4.1 Microsoft Windows 支持诊断工具（MSDT）远程代码执行漏洞

Microsoft Windows 支持诊断工具（MSDT）是一种 Windows 系统工具，可以帮助您诊断和解决 Windows 系统中出现的问题。它包含了大量的诊断工具和修复程序，可以帮助您解决各种问题，如蓝屏错误、系统崩溃、网络连接问题等。

攻击者可通过恶意 Office 文件中远程模板功能从服务器获取恶意 HTML 文件，通过‘ms-msdt’URI 来执行恶意 PowerShell 代码。该漏洞在宏被禁用的情况下，仍能通过 MSDT（Microsoft Support Diagnostics Tool）功能执行代码，将恶意 doc 文件另存为 RTF 格式时，无需打开文件，通过资源管理器中的预览选项卡即可在目标机器上执行任意代码。影响范围：Microsoft Office 2013、2016、2019 等主流版本。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2022-30190 |
| CVSS 3.1 | AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 漏洞评分 | 7.8 |
| 预警日期 | 2022-5-31 |

### 4.4.2 Microsoft Exchange Server 远程代码执行漏洞

Microsoft Exchange Server 是一种流行的电子邮件和日历应用程序，企业和组织使用它来管理他们的电子邮件通信。它是 Microsoft Server 产品线的一部分，该产品线包括其他服务器应用程序，例如 Active Directory、Lync 和 SharePoint。Exchange Server 提供多种功能，包括支持电子邮件、日历、联系人等。

CVE-2022-41082 是一个远程命令执行漏洞，要成功利用该漏洞必须先经过身份认证，之后即可利用一个网络调用来触发恶意程序代码。被微软列为重大（Critical）漏洞，经微软证实，黑客们利用 ProxyNotShell 漏洞，在被攻击的 Exchange 服务器上部署了 China Chopper web shell 恶意脚本。影响范围：Microsoft Exchange Server 2013、2016、2019 等主流版本。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2022-41082 |
| 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 | 2022-9-30 |

### 4.4.3 Spring Framework 任意文件写入漏洞

Spring Framework 是 Java 平台的应用程序框架和控制反转容器。该框架的核心功能可供任何 Java 应用程序使用，但也有用于在 Java Enterprise Edition (Java EE) 平台之上构建 Web 应用程序的扩展。Spring 为现代基于 Java 的企业应用程序提供了一个全面的编程和配置模型——在任何类型的部署平台上。

攻击者利用该漏洞可以在未授权的情况下，通过发送数据包，在目标服务器上写入任意文件，例如通过漏洞将 WebShell 写入目标服务器，然后通过访问 WebShell 来执行命令，进而获取整个服务器的权限。影响范围：3.0.0.M3 <= Spring Cloud Function <=3.2.2。

| | |
|---|---|
| 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 | 2022-3-30 |

### 4.4.4 Google Chrome 远程代码执行漏洞

谷歌浏览器是由谷歌开发的网络浏览器。它适用于台式机和移动设备，允许用户浏览互联网和访问范围广泛的在线服务和应用程序。Chrome 以其速度、安全性和对广泛的网络标准和技术的支持而闻名。它是世界上最流行的网络浏览器之一，每天有数百万人使用。

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。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2022-3723 |
| CVSS 3.1 | AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 漏洞评分 | 8.8 |
| 预警日期 | 2022-10-28 |

### 4.4.5 F5 BIG-IP iControl REST 身份验证绕过漏洞

F5 BIG-IP 是 F5 Networks 生产的一系列网络设备。这些设备提供一系列与网络和应用程序性能相关的服务，包括负载平衡、流量管理和应用程序安全。BIG-IP 设备通常被大型组织用来提高其网络和应用程序的性能、可靠性和安全性。

CVE-2022-1388 该漏洞是一个身份验证绕过漏洞，未经身份验证的攻击者利用此漏洞可以通过管理端口或利用自身 IP 对 BIG-IP 系统进行网络访问绕过身份验证,并且可以任意执行系统命令、创建或删除文件以及禁用 BIG-IP 上的服务。影响范围：16.1.0 - 16.1.2、15.1.0 - 15.1.5、14.1.0 - 14.1.4、13.1.0 - 13.1.4、12.1.0 - 12.1.6、11.6.1 - 11.6.5。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2022-1388 |
| 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 | 2022-5-6 |

### 4.4.6 Fastjson 反序列化漏洞

Fastjson 是一个 Java 语言编写的高性能功能完善的 JSON 库。它采用一种“假定有序快速匹配”的算法，把 JSON Parse 的性能提升到极致，是目前 Java 语言中最快的 JSON 库。Fastjson 接口简单易用，已经被广泛使用在缓存序列化、协议交互、Web 输出、Android 客户端等多种应用场景。

Fastjson 使用黑白名单用于防御反序列化漏洞,在特定条件下使用该漏洞可绕过默认 autoType 关闭限制，攻击远程服务器。影响范围：特定依赖存在下影响 ≤1.2.80。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2022-25845 |
| 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 | 2022-5-23 |

### 4.4.7 Spring Cloud Gateway 远程代码执行漏洞

Spring Cloud Gateway 是基于 Spring Framework 和 Spring Boot 构建的 API 网关，它旨在为微服务架构提供一种简单、有效、统一的 API 路由管理方式。当启用和暴露不安全的 Gateway Actuator 端点时，使用 Spring Cloud Gateway 的应用程序容易受到代码注入攻击。远程攻击者可以发出恶意制作的请求，成功利用该漏洞可以导致代码执行。影响范围：Spring Cloud Gateway < 3.1.1、Spring Cloud Gateway 3.0.0 -3.0.7、Spring Cloud Gateway 其他已不再更新的版本。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2022-22947 |
| CVSS 3.1 | AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H |
| 漏洞评分 | 10 |
| 预警日期 | 2022-3-2 |

### 4.4.8 Polkit 权限提升漏洞

Polkit 是 Linux 操作系统的一个组件，它使非 root 用户能够执行通常需要 root 权限的管理任务。它通过定义一组规则来实现这一点，这些规则确定何时允许特定用户或用户组执行特定任务。当用户尝试执行特权操作时，Polkit 会检查规则以查看用户是否具有执行管理任务的能力，而无需以 root 用户身份登录，这样可以更轻松地管理系统设置并提高系统安全性，无需切换到 root 用户就能轻松地管理他们的系统。

CVE-2021-4034 是由于 pkexec 无法正确处理调用参数，从而将环境变量作为命令执行，具有任意用户权限的攻击者都可以在默认配置下通过修改环境变量来利用此漏洞，从而获得受影响主机的 root 权限。影响范围十分广泛。

| | |
|---|---|
| 漏洞类型 | 权限提升 |
| 漏洞编号 | CVE-2021-4034 |
| 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 | 2022-1-27 |

### 4.4.9 Apache Struts2 远程代码执行

Apache Struts 2 是用于开发 Java EE Web 应用程序的开源 Web 应用程序框架。它使用并扩展了 Java Servlet API 以鼓励开发人员采用模型-视图-控制器 (MVC) 架构。Struts 2 旨在使开发可扩展、可维护和灵活的 Web 应用程序变得更加容易。它建立在流

行的开源 Apache Commons 组件之上，为开发人员提供了一组可重用的核心组件，用于构建 Web 应用程序。导致该漏洞的原因是对 S2-061 修复不够完整，当开发人员使用%{……}语法强制 OGNL 解析时，还是会有一些特殊的标签属性会被二次解析，攻击者可以向受害主机发送恶意的 OGNL 表达式执行任意代码。影响范围：2.0.0 <= Apache Struts <= 2.5.29。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2021-31805 |
| 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 | 2022-4-14 |

### 4.4.10 Atlassian Confluence RCE 漏洞

Atlassian Confluence 是一个协作平台，它可以帮助团队成员更好地协作、沟通和共享信息。它提供了一个简单易用的界面，允许团队成员创建和编辑文档、添加图片和视频等，并能够方便地与其他人共享这些内容。此外，Confluence 还提供了许多其他功能，例如项目管理、知识库管理和团队博客等，可以帮助团队成员更好地管理信息和提高协作效率。

该漏洞允许在未经身份验证的情况下，通过发送恶意的 Web 请求注入命令，实现在受影响的 Confluence Server 或 Data Center 实例上执行任意代码。当时影响范围很广。

| | |
|---|---|
| 漏洞类型 | 远程代码执行 |
| 漏洞编号 | CVE-2022-26134 |
| 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 | 2022-6-4 |


2022 年网络空间安全漏洞分析研究报告显示，漏洞数量仍然不容忽视，但相比往年多数漏洞已经得到了有效的解决，CNVD 披露的漏洞数量出现了下降趋势。可见技术发展、相关政策法规的完善和安全机制的建立在漏洞治理方面发挥了重要作用。另外，企业组织也需要重视漏洞管理工作，优先修补和防护中高及严重风险漏洞，优化漏洞管理计划的成熟度和有效性。保护外部接入点，加强对网络边界的审查和保护，监控和保护物联网设备、工业控制系统等非传统网络设备的安全。评估操作系统、智能设备、安全产品和数据库的安全性，使用安全设计原则保证系统安全性。校验输入数据，建立有效的数据防泄漏系统。

通过对 2022 年 CVE 发布的高危漏洞统计分析可知，漏洞依然集中在传统厂商的设备和产品中，且受影响的平台大致可分为五类，其中硬件设备平台占据首位。这说明传统厂商的设备和产品依然是高危漏洞的主要载体，这些设备和产品还存在较高的安全风险，用户在使用这些设备和产品时应该注意加强安全防护，尤其是硬件设备，因为这类设备的漏洞更难以修复。2 月份共披露了高危漏洞 22 个，位居全年第一，其中大约 17%的高危漏洞存在公开 POC。公开 POC 可能会为攻击者提供便利条件，使其能够更快地研发攻击工具。大多数漏洞都是可以被远程利用的，只有很少一部分漏洞可以被本地利用。这意味着，系统的网络安全防护措施尤为重要。在前 100 个漏洞中，远程代码执行漏洞、SQL 注入漏洞、命令注入漏洞是当前网络安全形势下最为严峻的威胁。为了确保网络安全，应该加强网络安全管理，健全安全技术，针对这些漏洞提供有效的防护措施。

2022 年漏洞预警多为主流操作系统，其中 Windows 系统漏洞和远程代码执行漏洞预警最多。还有一些关键基础设施如 OpenSSL 和 Vmware 的漏洞也出现在其中。这类漏洞也是 APT 攻击者的重点，操作系统类漏洞的影响面很大，因为它们可能涉及到操作系统的核心功能，对整个系统的安全造成威胁。如果攻击者成功利用这些漏洞，就有可能会爆发蠕虫病毒传播事件或者勒索事件，对目标网络和信息系统造成严重影响。对于仍旧存在的各种漏洞事件，建议企业、组织加强安全技术研究和投入，建立完善的安全防护体系，有效地发现和堵塞漏洞，以减少网络空间安全漏洞的发生。

## 5.1 安全防护建议

归纳 2022 网络空间安全态势和应对措施，主要分为如下几点：

**1、攻击形式多样且多层次，应不断强化安全防护措施，建立全面的安全防护体系。**纵观近年所披露的安全事件，不难发现攻击手段在不断升级，攻击路径也是多种多样，涵盖了信息系统整个生命周期。在 2022 年 2 月，向日葵软件的 Windows 版本发现存在远程代

码执行漏洞。攻击者通过向日葵的 Web 服务随机端口获取 Cookie CID，构造恶意请求执行命令并获取服务器控制权限。向日葵的远程控制特性使得很多人将其作为后台进程运行，如果暴露在公网上则会造成巨大危害。疫情期间增加的远程办公场景和远程控制软件使用增加了系统被黑客攻击的风险。远控黑产团伙多次利用这个漏洞攻击企业主机和个人电脑。

同样在 2 月发生的 NPM 存储库供应链攻击事件表明，软件供应链攻击已经出现了新的攻击手段，攻击者在不断提高攻击技能，使防御变得更加困难。这次攻击者使用了自行编写的 Python 代码和 Selenium 等 Web 测试工具，来模拟新用户创建并绕过了其中的一次性验证密码（OTP），从而将近 800 个恶意 NPM 包自动批量上传到 NPM。攻击者通过使用多个用户名分发恶意软件包，从而增加感染的机会。另外由于很多 NPM 开发者的邮箱域名都已过期但还用来登录，在没有双重身份认证的情况下，黑客只需要把域名买下来就可以劫持账户，同样可以在开源项目中注入恶意代码。

今年还出现了与 Log4j 远程代码执行漏洞不相上下的 Spring4Shell（CVE-2022-22965），该漏洞是由于 JDK9 及以上版本引入对模块化的支持从而绕过了 CVE-2010-1622，结合 Struts2 S2-020 在 Tomcat 8 下的命令执行的方法，对 Tomcat 的处理请求日志管道（AccessLogValve）进行改写，导致当前请求触发记录日志，并按照特定方式生成了 JSP 文件。尽管该漏洞利用存在诸多限制，但根据相关数据显示，受漏洞影响组织中六分之一已成为攻击者的目标。在漏洞爆发一周内就检测到了 37000 次攻击。Spring 作为应用量庞大的的 Java 开发框架，出现漏洞将会导致许多应用程序受到影响。这可能会导致严重安全问题并给企业带来巨大的经济损失。

由此可见，原有单一安全手段已无法满足变化的网络威胁，应不断强化信息系统防护措施，构建立体防御体系。

**2、定期安全培训，提升人员安全意识**。除采取的安全措施外，安全意识同样严重影响信息系统的安全。西北工业大学官方公众号 6 月 22 日发布公开声明，该校电子邮件系统遭受网络攻击，对学校正常教学生活造成负面影响，此次事件初步判定为境外黑客组织发起的攻击。境外的黑客组织和不法分子向学校师生发送包含木马程序的钓鱼邮件，企图窃取相关师生邮件数据和公民个人信息，给学校正常工作和生活秩序造成重大风险隐患。

今年 2 月 24 日，俄乌战争打响，在此背景下，两国针对性的网络攻击事件频发，3 月中旬，来自世界各地的至少 3 个不同的高级持续威胁 APT 组织发起了鱼叉式网络钓鱼活动，利用正在进行的俄乌战争作为诱饵，分发恶意软件和窃取敏感信息，这些 APT 攻击中的攻击者使用了各种诱饵，例如创建假新闻、社交媒体活动、垃圾邮件、虚假诱饵网站以及其他形式的诱饵，来诱惑受害者下载恶意软件、文档或点击恶意链接。其中许多诱饵文档利用远程模板注入执行宏代码等方法渗透目标组织，然后发起恶意软件攻击。

由此可见，人是影响系统运行的重要变量，人员操作严重影响信息系统的网络安全，

所以定期对人员进行安全培训，避免出现终端用户安全意识薄弱导致终端设备安全基线降低；内网应用被网络钓鱼、漏洞利用、凭证窃取等方式攻陷；内部数据通过即时通信和电子邮件等工具被泄露；甚至是针对办公网络的 APT 攻击等等，只有长期保持并不断强化安全意识，才能有效提升网络安全总体能力。

**3、分类处置安全漏洞，及时妥善处理内部安全隐患。**近年来，公开披露的漏洞数量逐年上升，大量漏洞情报来袭，由于漏洞数量多、漏洞危害有大有小、漏洞影响范围不一等问题存在，如何有效应对成为令运营者头疼的问题。基于收集的安全数据，我们认为至少应坚持以下三项原则，以有效应对该问题。

一是应重视漏洞情报工作，务必以最快的速度反应。公开披露漏洞情报，对防御和攻击工作都有帮助，防御者依靠漏洞情报更新防御，而攻击者则依靠情报研究攻击手法，所以不更新防御等同于放弃安全。

二是对业务分级分类进行处理。已知漏洞情报数量较多，运营者可通过业务分级筛选，以突出重点，便于进一步加快处置速度。

三是关注漏洞的综合影响，分类处理漏洞。安全漏洞量化指标中，除漏洞危害、影响范围、利用复杂度外，可利用性同样是重要关注点。以上量化指标均处于高危的漏洞，运营者应快速妥善处置。

**4、完善的漏洞管理措施是整个漏洞防护体系中最重要的一环，作为企业安全建设的重要工作，需要一个清晰的、体系化的漏洞管理思路，以提高漏洞管理水平**。为此，天融信提出了网络安全漏洞全生命周期闭环管理解决方案。方案以天融信漏洞管理平台为主要载体，可实施“六步走”策略，从多角度覆盖漏洞治理全流程，实现漏洞收集、验证、处置、跟踪的闭环管理效果。

第一步、对资产进行全量采集与发现，并通过自动化工单流转建立标准化资产管理流程。

第二步、收集知名漏洞库、开源社区、安全论坛、供应商官方网站等披露的漏洞信息，通过与存量资产关联，第一时间感知资产风险。

第三步、结合人工、自动化工具对漏洞有效性、真实性进行验证。优先修复风险等级高的漏洞，提升漏洞修复效率。

第四步、对修复后的漏洞持续跟踪监测，经二次扫描研判，视情况对防范措施做进一步改进。

第五步、建立企业漏洞挖掘众测机制，调动内、外部安全专家积极性，发挥其技术实力，更好发现自有业务系统和产品安全风险。

第六步、建立漏洞发布内部审核机制，确认所有公开漏洞已被修复且无重大影响。


图 16 安全防护方案架构图

## 5.2 漏洞态势展望

随着软件的复杂度以及企业和开发者对安全的重视度增加，包括开发和不断完善自动化安全审计流程、进行更多的内部安全测试、使用安全开发方法和工具以及提高开发人员的安全意识等。最终的漏洞数量可能会呈现下降趋势，对于企业办公系统来说，Windows、Linux、Mac 属于主流操作系统，这三个系统的漏洞数量可能不会降低，其中 Windows 在野利用漏洞依旧居高不下，大多数为权限提升漏洞。网络活动都是以人为载体的，除了及时安装最新补丁之外，还需要定期培训，提高人员的安全操作意识。

在近两年，Microsoft Exchange Server 出现了较多的在野利用漏洞，由于 Microsoft Exchange Server 是基础设施，攻击它可以为攻击者带来更多的利益，预计在 2023 年会有更多的此类漏洞出现。同时，随着 Adobe Flash 和 Internet Explorer 生命周期的结束，攻击者和安全研究人员可能会把更多的注意力放在使用更广泛的浏览器（如 Google Chrome、Apple Safari 和 Mozilla Firefox）上。JavaScript 引擎的攻击面很大，大多数漏洞来自各大浏览器的 JavaScript 引擎。预计在 2023 年也会有更多的浏览器在野漏洞出现。

REST API 的普及导致越来越多应用程序对外开放了 API 接口，但这也带来了新的安全风险，API 接口的设计容易存在缺陷，身份验证也可能被绕过。因此，API 安全将持续成为网络空间安全的一大威胁。随着技术的不断发展，攻击者可能会利用人工智能和机器学习技术来更有效地发现和利用漏洞，并且也可能会更加关注云环境和物联网设备缺陷挖掘。为了保护国家信息基础设施不受恶意攻击，政府和监管机构可能会出台更严格的软件安全法规。为了应对这些挑战，客户应加强攻击面管理，及时发现和修复漏洞，并做好威胁检

测和响应，以便在攻击者得逞之前及时阻止攻击。

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。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。