天融信 TOPSEC
证券代码：002212
1995-2021 天融信

可信网络 安全世界

2021年
网络空间安全漏洞
调研分析报告

天融信科技集团

2022年1月

目录

第一章 前言

2021 年是中华人民共和国十四五规划开启的第一年，在十四五规划中，网络安全作为社会发展的重要一环，再次被作为重点提起，中央强调要健全国家网络安全法律法规和制度标准，加强重要领域数据资源、重要网络和信息系统安全保障。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全风险评估和审查。加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源的能力。

在网络安全的发展过程中，围绕的核心向来都是漏洞，漏洞的产生造就了众多危害网络安全，乃至用户人身安全的事件产生。

软件产品由于开发及设计等各方面原因，存在安全漏洞在所难免。天融信阿尔法实验室特发布《2021 年网络空间安全漏洞调研分析报告》，旨在通过对漏洞发展趋势的研究帮助广大企事业客户、安全运维人员等应对严峻的漏洞威胁。

本报告重点内容共分两个部分，第一部分为 2021 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,2020 年共披露漏洞 20248 枚，2021 年共披露漏洞 17702 枚,同比降低 13%。2021 年高危漏洞类型分布相对集中,表现为代码执行类型的漏洞拥有较大的占比，这类高危漏洞对网络空间安全的威胁远远高于其他类型漏洞，这种高威胁漏洞数量的占比预示了当前严峻的网络安全态势。

第二部分为天融信 2021 年度高危漏洞预警情况概述,在 2021 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、和产生威胁的因素从中挑出了排名前十的漏洞。2021 年度重点漏洞含 Apache Log4j2 远程代码执行漏洞、Microsoft Windows Active Directory 域服务权限提升漏洞、Weblogic 远程代码执行、ExchangeServer 远程代码执行、Windows Defender 远程代码执行漏洞等。其中最知名的漏洞莫过于 Apache Log4j2 远程代码执行漏洞，实验室第一时间监测到漏洞后，进行漏洞复现，第一时间进行源码层面的原理分析，并给出临时缓解方案，且于当日再次拦截到补丁绕过的信息，迅速进行人工复现分析，快速整理给出了完整的漏洞应急处理方案，最终将该方案提供给每一位客户。最后是总结部分，虽然安全漏洞数量整体呈下降趋势，但高威胁漏洞数量和占比依旧高居不下，漏洞影响面逐步扩大，关键协议、服务器中间件、通用开发框架及操作系统的漏洞威胁日益严峻，严重影响各类关键信息系统基础设施，基于漏洞引发的网络安全威胁应引起高度警惕。

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的赋能。

第二章 CNVD 漏洞库安全漏洞调研概况

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 2021 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

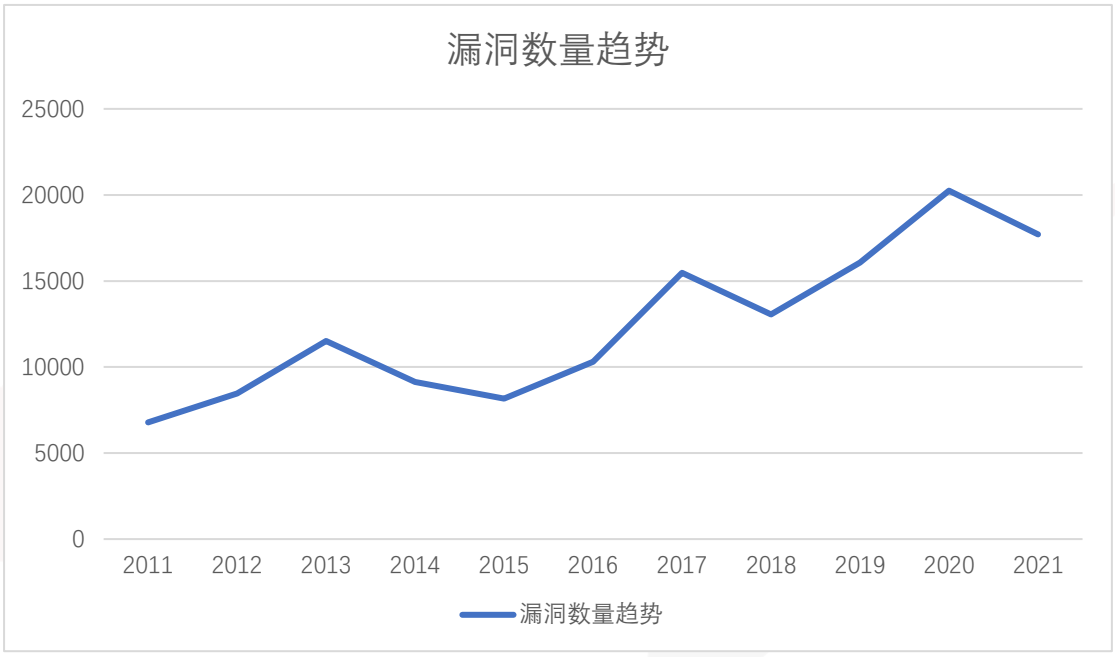

图 1 近十年漏洞数量走势图(数据来自于 CNVD)

2.1 漏洞威胁等级统计

根据 2021 年 1-12 月漏洞引发威胁严重程度统计，其中低危漏洞 33.5%，中危漏洞 57.3%，高危漏洞 9.2%。

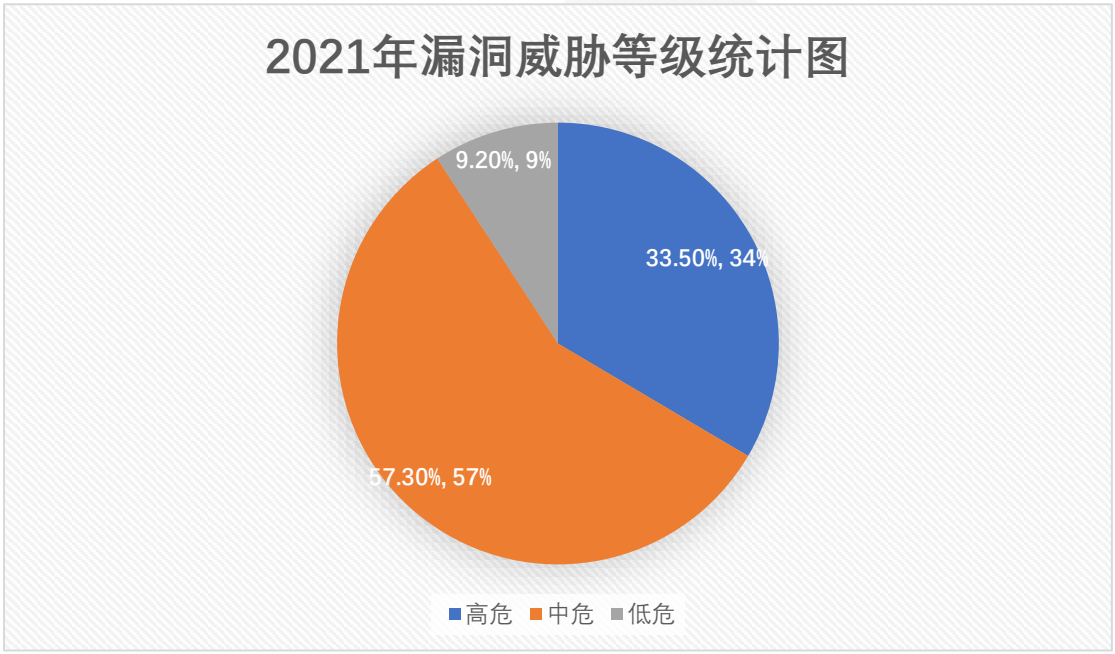

图 2 2021 年收录漏洞按威胁级别统计(数据来自于 CNVD)

2.2 漏洞利用攻击位置统计

根据 2021 年 1-12 月漏洞引发威胁统计，其中远程攻击占比约为 86.3%，本地攻击约占 12.9%，其他攻击为 0.8%。由此可见远程攻击是主要的漏洞攻击的手段，远程攻击也是我们主要防范的漏洞攻击手段。

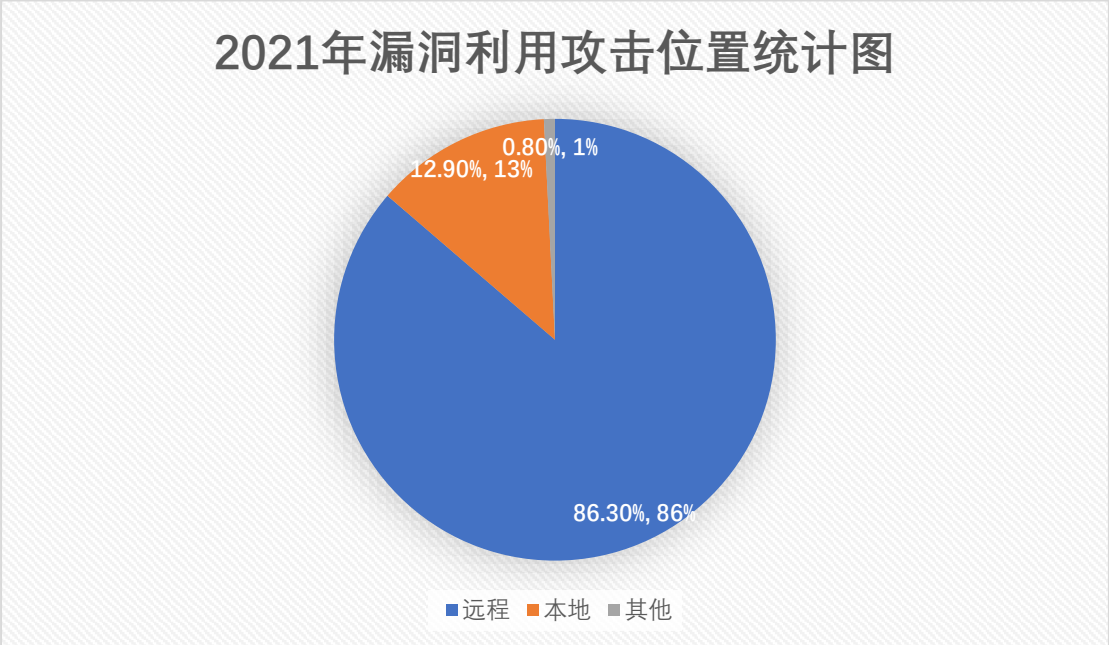

图 3 2021 年收录漏洞利用的攻击位置统计（数据来自于 CNVD）

2.3 漏洞影响对象类型统计

根据 2021 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：分别是操作系统漏洞、应用程序漏洞、 WEB 应用漏洞、数据库漏洞、网络设备漏洞、安全产品漏洞、智能设备漏洞、区块链公链漏洞、区块链联盟链漏洞、工业控制系统漏洞。其中应用程序漏洞 56.3%， WEB 应用漏洞 22.3%，操作系统漏洞 9.9%，网络设备漏洞 6.7%，智能设备漏洞 0.8%,区块链公链漏洞 0.3%,安全产品漏洞 1.9%，数据库漏洞 1.8%，工业控制系统漏洞 0.1%。

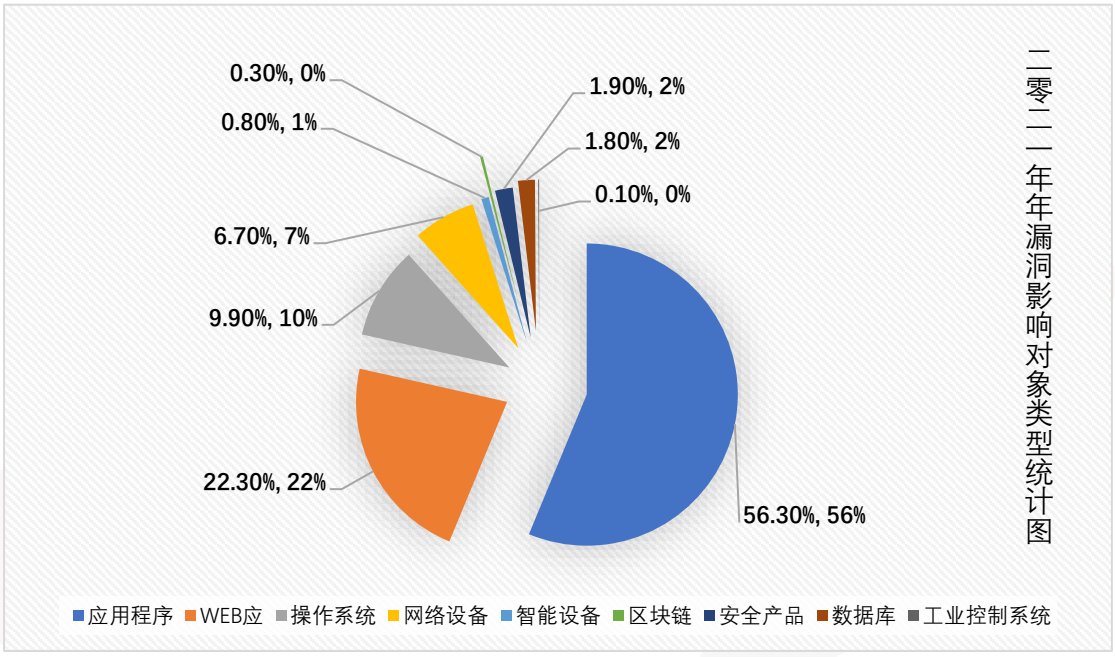

图 4 2021 年漏洞影响对象类型统计(数据来自于 CNVD)

2.4 漏洞产生原因统计

根据 2021 年 1-12 月漏洞产生原因的统计，设计错误导致的漏洞占比 52.3% 屈居首位，紧跟其后的是输入验证错误导致的漏洞 28.9%位居第二，接着是边界条件错误导致的漏洞占比 7.9%位居第三。后面的意外情况处理错误，其他错误，访问验证错误，未知错误，竞争错误，配置错误，环境错误。分别为 4.2%、2.6%、2.2%、0.8%、0.6%、0.5%、0.1%。

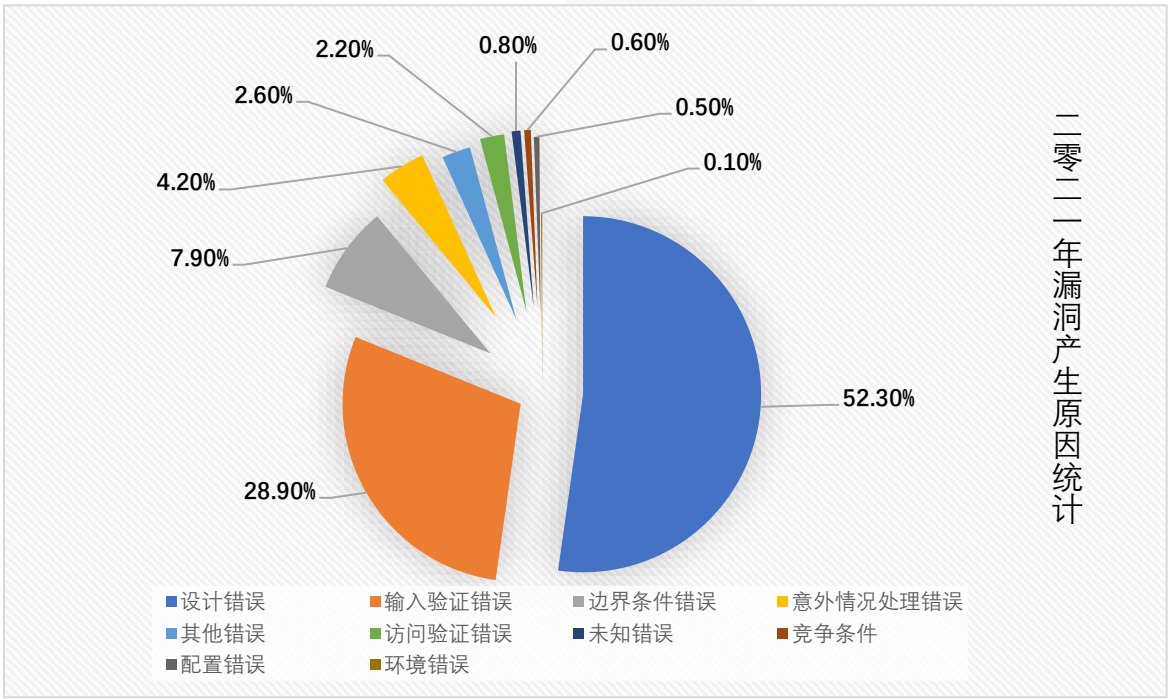

图 5 2021 年漏洞产生原因统计(数据来自于 CNVD)

2.5 漏洞引发威胁统计

根据 2021 年 1-12 月漏洞引发威胁统计，未授权的信息泄露占比 29.2%居首位，管理员访问权限获取占比 25.2%位居第二，拒绝服务占比 16.1%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 13.1%、10.4%、4.4%、1.5%。

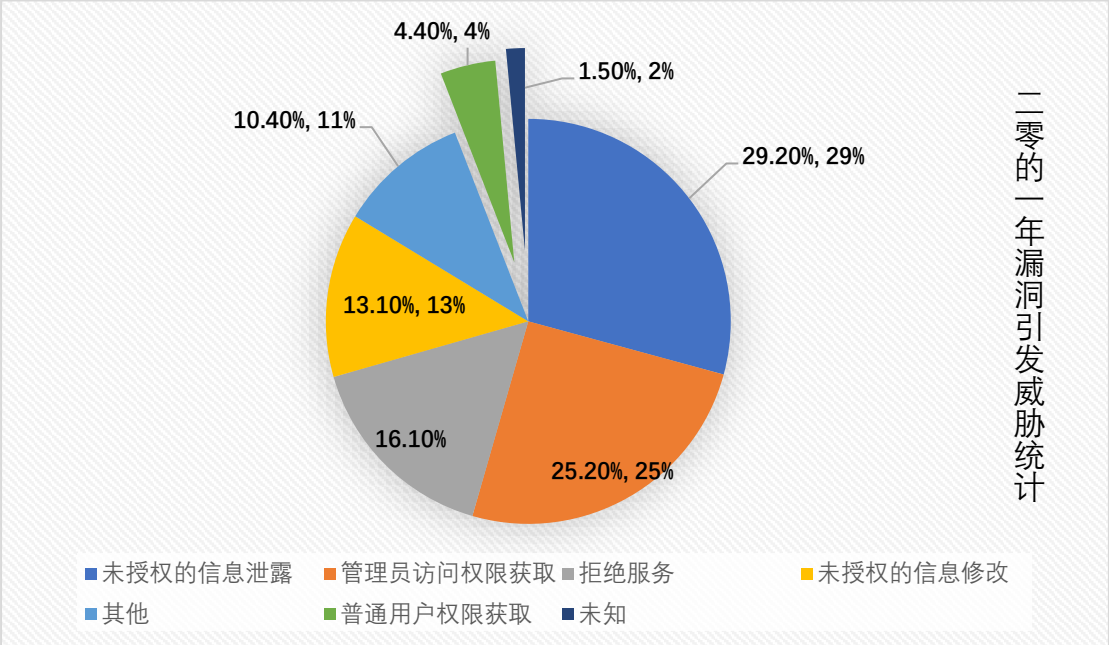

图 6 2021 年漏洞引发威胁统计(数据来自于 CNVD)

2.6 漏洞增长趋势

通过 CNVD 漏洞信息库对 2020、2021 漏洞公开数据显示，2020 年一共披露漏洞 20248 枚，2021 年一共披露漏洞 17702 枚。同比减少 13%，2021 年高危漏洞 5134 枚，同比 2020 年减少 26.32%，2021 年中危漏洞 10548 枚，同比 2020 年减少 2.42%，2021 年低危漏洞 2020 枚，同比 2020 年减少 14.76%。

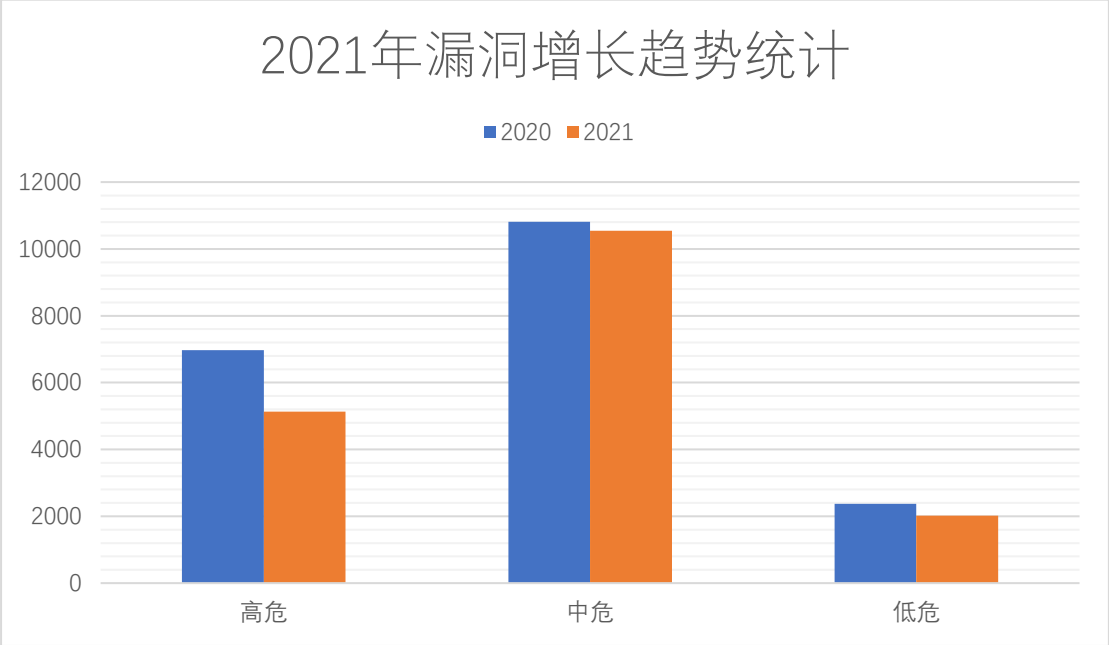

图 7 2021 年漏洞增长趋势统计（数据来自 CNVD）

第三章 CVE 漏洞库安全漏洞调研概况

通过对 CVE 在 2021 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 Adobe、苹果及 Google。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 PC 端平台漏洞 43%，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 26 个，位居全年第一。在 TOP100 漏洞中大约有 4%的高危漏洞存在公开 POC，这一数据占比不高，但公开 POC 就给攻击者提供了便利条件，一旦被攻击者率先掌握了漏洞的利用方式，并以此实现攻击工具，将对相关的软硬件设备造成重大的安全危害，对用户形成威胁。为避免类似事件，需由软硬件厂商及安全厂商携手以建立良好的安全生态。

从攻击途径看可被远程利用的漏洞占比约为 47%，本地利用的漏洞约占 53%，来自互联网的漏洞和本地利用的漏洞数量平分秋色，二者都要给予相同的重视。在 TOP100 高危漏洞中，远程代码执行类型的漏洞共占比 25%。漏洞类型分布相对集中,表现为远程代码执行类类型的漏洞和本地利用的代码执行漏洞占比为绝大多数，这类高危漏洞对网络空间安全的威胁远远高于其他类型漏洞，这种高威胁漏洞数量的占比预示了当前严峻的网络安全态势。
具体统计分析结果如下:

3.1 漏洞影响厂商分布情况

根据 2021 年 1-12 月 CVE 披露漏洞危害程度前 100 例所影响的厂商情况进行统计，前三名分别是 Adobe、苹果及 google。其中 Adobe 厂商的产品占比达到 31%，苹果的产品占到 18%，Google 的产品共占 12%。

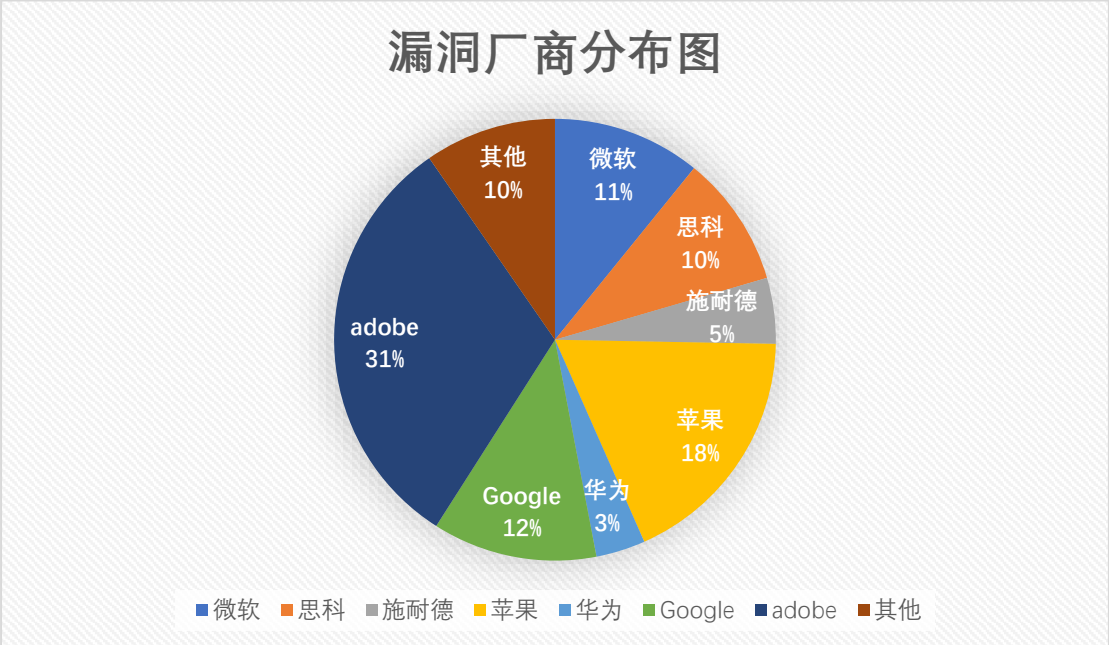

图 8 漏洞厂商分布图(数据来自于 CVE)

3.2 高危漏洞披露时间趋势图

根据 2021 年 1-12 月 CVE 披露漏洞危害程度前 100 例披露时间进行统计，在 2021 年全年中，2 月份披露 26 个 TOP100 漏洞占比 26%位居第一，4 月与 3 月份分别披露 14 个漏洞并列第二，6 月和 9 月各披露 11 个漏洞并列第三。

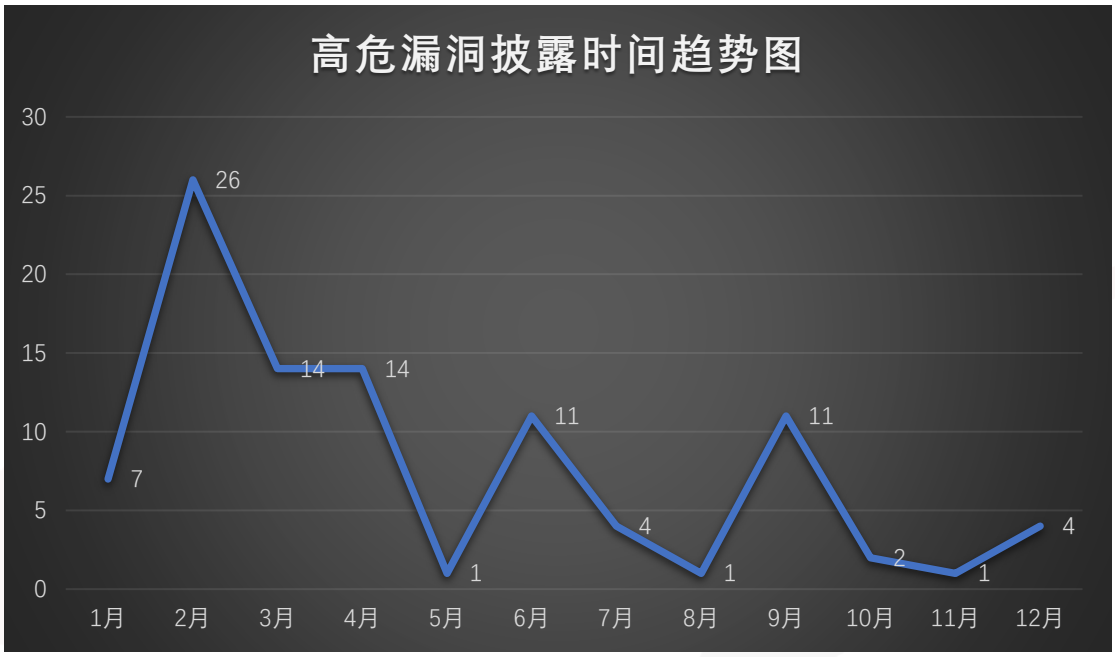

图 9 高危漏洞披露时间趋势图(数据来自于 CVE)

3.3 攻击途经概况

根据 2021 年 1-12 月 CVE 披露漏洞危害程度前 100 例攻击途径进行统计，其中来自远程攻击占比约为 47%，本地攻击约占 53%。今年本地利用的漏洞数量占比提升，环比增长约 32%，但是远程利用的漏洞数量依旧占比不低，可见在未来的工作中，来自本地和远程的攻击和利用都将是防护重点。

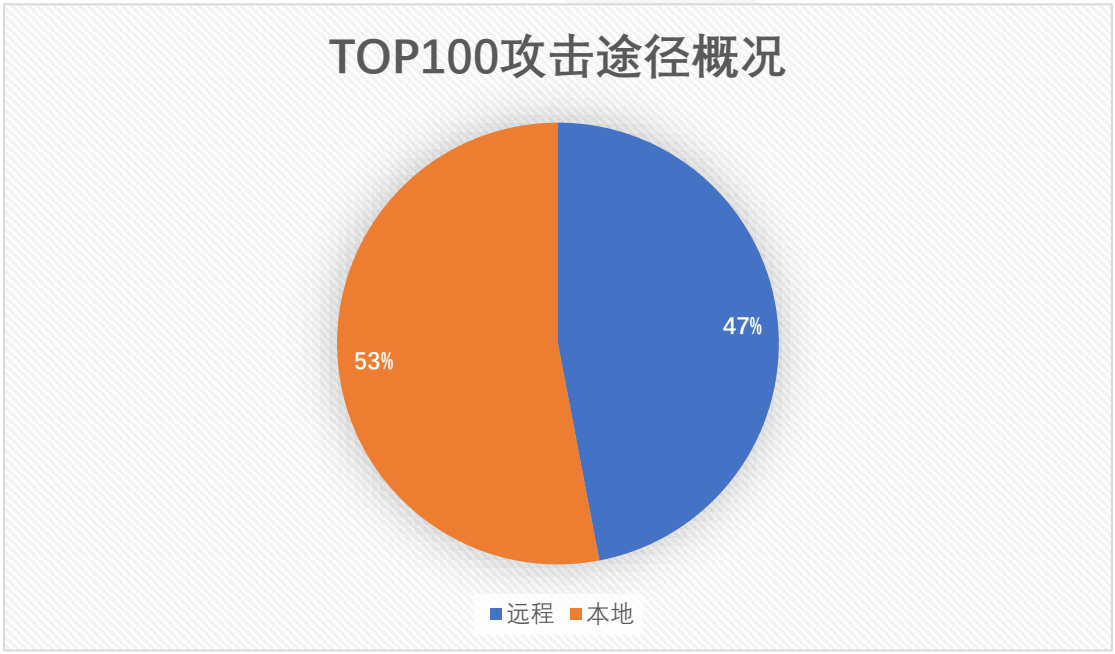

图 10 TOP100 攻击途径概况(数据来自于 CVE)

3.4 漏洞影响平台分类

根据 2021 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 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 PC 端平台漏洞 43%，移动端平台漏洞 29%，硬件设备平台漏洞 15%，跨平台漏洞 8%，其他漏洞 5%。

图 11 TOP100 漏洞平台分类(数据来自于 CVE)

3.5 漏洞类型统计概况

根据 2021 年 1-12 月 CVE 披露漏洞危害程度前 100 例类型进行统计，其中本地代码执行漏洞占比最多，以 39%位居首位，而远程代码执行占比 25%、权限提升占比 11%、信息泄露占比 4%、拒绝服务占比 2%、命令执行占比 2%，身份验证失效占比 2%，其他漏洞占比 15%

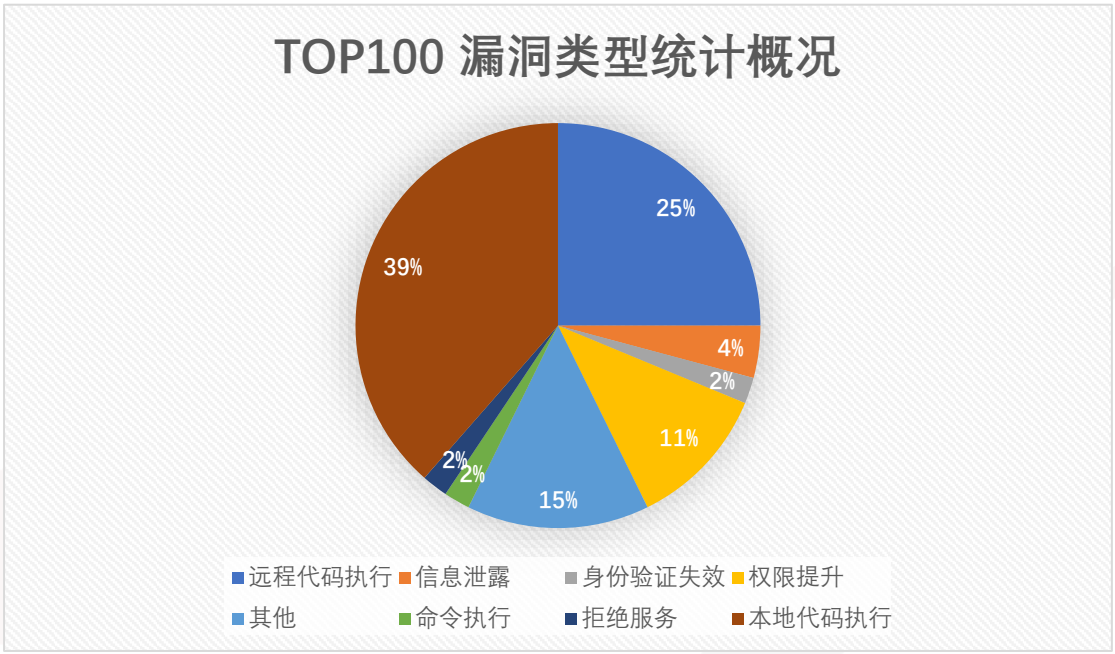

图 12 TOP100 漏洞类型统计概况(数据来自于 CVE)

3.6 TOP100 POC 公开情况统计

根据 2021 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 96%，公开 POC 的仅有 4%。

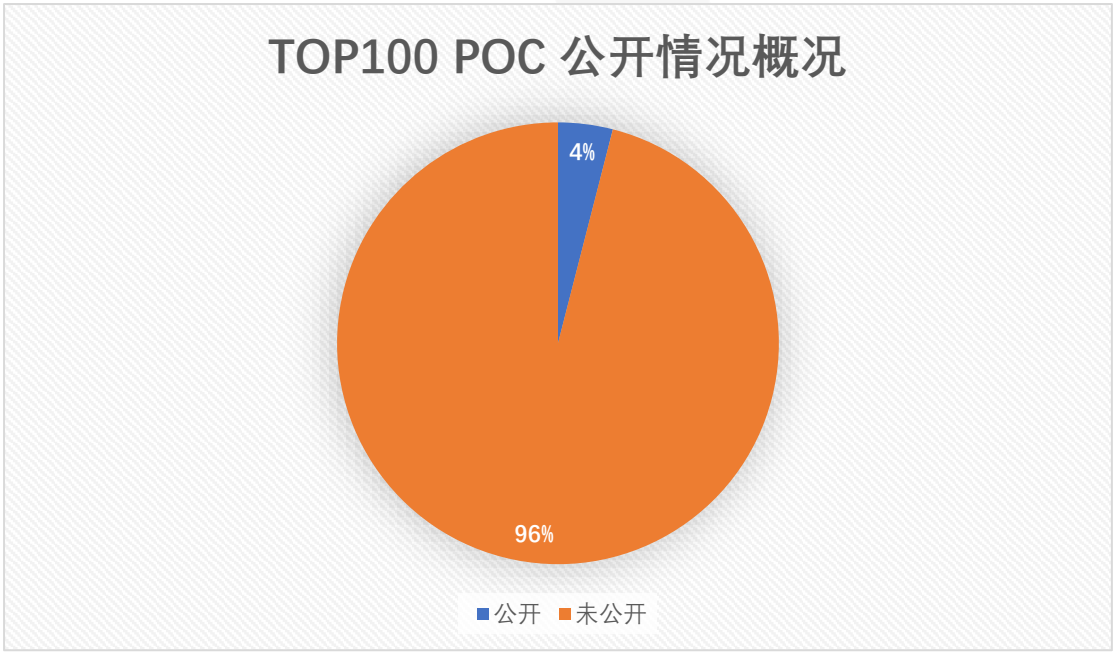

图 13 TOP100POC 公开情况概况(数据来自于 CVE)

第四章 漏洞预警统计情况

天融信阿尔法实验室在 2021 年共监测发现各类漏洞信息约 46316 条，数据来源为社交媒体、专业安全信息网站、程序员社区、厂商公告。由自动智能筛选后留存高危漏洞信息共计 462 条，经人工研判后发布高危漏洞风险提示通告共计 66 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。2021 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。Weblogic、Log4j2、Xstream、Vmware 等关键基础设施漏洞也是受关注度较高的方向。

2021 年预警的漏洞中，代码执行类漏洞占比最高，达到 55%。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 2021 年内发布的 66 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 22 次，占比约 33%，针对 Apache 的为 8 次，占比 12%，位居第二名，针对 Vmware 厂商的漏洞预警为 7 次，占比约 11%位居第三名。

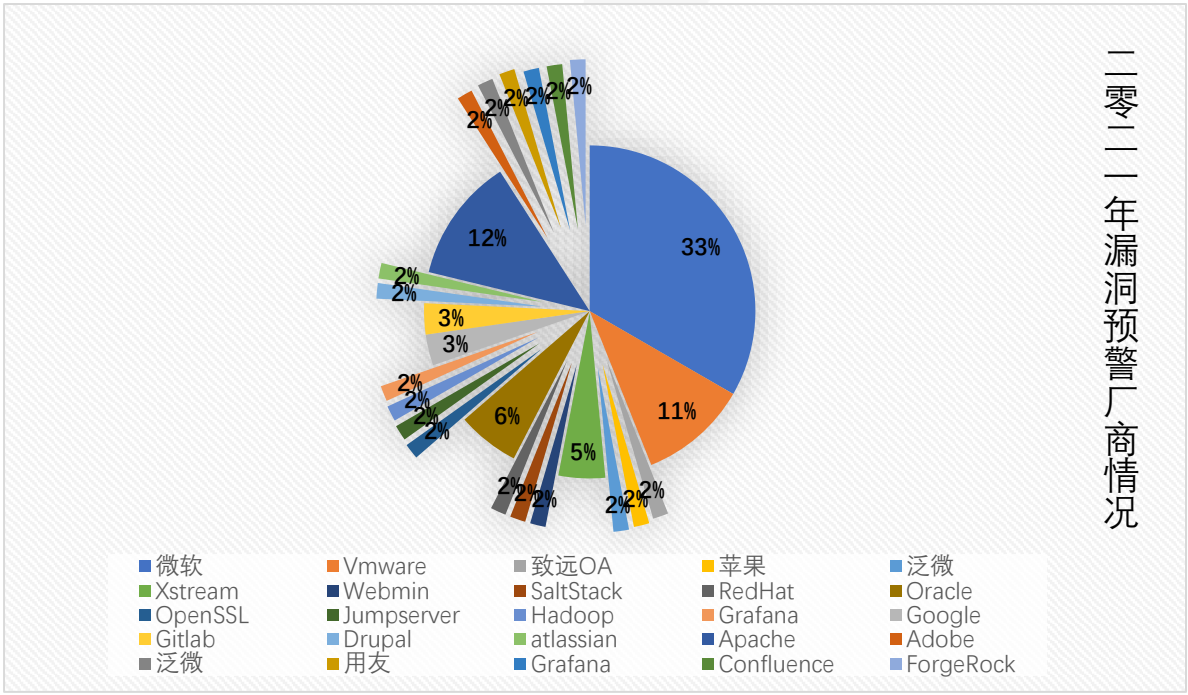

图 14 2021 年漏洞预警厂商情况

4.2 漏洞威胁情况

在 2021 年发布的 66 条漏洞通告中，所通告的漏洞可分为 13 大类，分别是远程代码执行漏洞、拒绝服务漏洞、未授权访问漏洞、任意文件上传、任意文件读取、命令执行漏洞、权限提升漏洞、信息泄露漏洞、SSRF 漏洞、CSRF 漏洞、路径遍历漏洞、身份绕过漏洞、XSS 漏洞，其中代码执行漏洞占 55%位于首位，权限提升漏洞占比 17%位于第二位、信息泄露漏洞占比 6%位于第三位

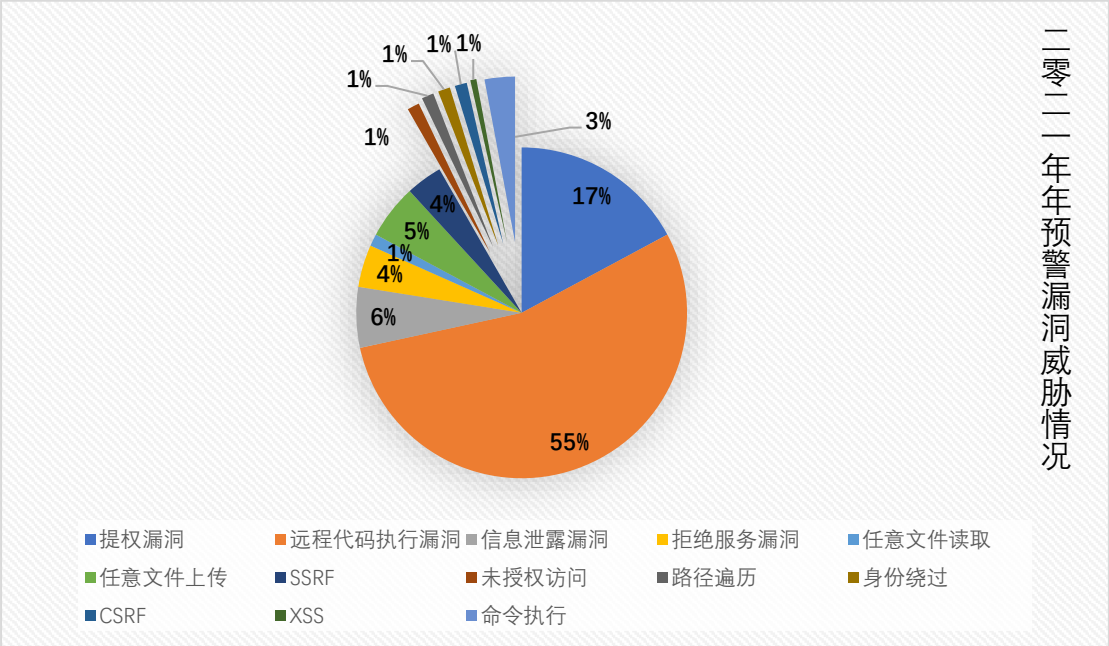

图 14 2021 年预警漏洞威胁情况

4.3 年度 TOP10 高危漏洞

本节内容筛选自天融信 2021 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，漏洞影响的范围广度进行排名，并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-2021-44228	Apache Log4j2 任意代码执行漏洞	Log4j2 某些功能存在递归解析功能，未经身份验证的攻击者通过发送特定恶意数据包，可在目标服务器上执行任意代码。该漏洞的影响版本 Apache Log4j 2.x < 2.15.0-rc2，该组件应用范围非常广泛，如：Apache Struts2、Apache Solr、

			Apache Druid 等开发框架及中间件中。从 Apache Log4j2 漏洞影响面查询的统计来看，影响多达 60644 个开源软件，涉及相关版本软件包更是达到了 321094 个，所以有人称这个漏洞是"核弹级",侧面说明了这个漏洞的危害。
NO.2	CVE-2021-2394	Weblogic 任意代码执行漏洞	CVE-2021-2394: 任意执行代码漏洞是一个二次反序列化漏洞，是 CVE-2020-14756 和 CVE-2020-14825 的调用链相结合组成一条新的调用链来绕过 weblogic 黑名单列表。攻击者可以在未授权的情况下通过 IIOP、T3 协议对存在漏洞的 WebLogic Server 组件进行攻击。成功利用该漏洞的攻击者可以接管 WebLogic Server。
NO.3	CVE-2021-2397 CVE-2021-2382	Oracle 任意代码执行漏洞	漏洞存在于 Oracle WebLogic Server 中，Oracle WebLogic Server 是一个 Java 应用服务器，它全面实现了 J2EE 1.5 规范、最新的 Web 服务标准和最高级的互操作标准。WebLogic Server 内核以可执行、可扩展和可靠的方式提供统一的安全、事务和管理服务。 这个漏洞披漏于 4 月 21 日，之所以严重是因为该漏洞影响范

			围涉及到 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 等众多版本。而且攻击者可以在未授权的情况下通过 T3 或 IIOP 协议发送恶意请求，最终接管服务器。
NO.4	CVE-2021-24074 CVE-2021-24094 CVE-2021-24086	Windows 的 TCP/IP 协议簇远程代码执行漏洞&拒绝服务漏洞	该漏洞的影响范围 Windows Server 2019、2016、2012 R2、2008 R2 等版本。漏洞产生于 Windows TCP/IP 的协议簇存在远程代码执行、拒绝服务漏洞，攻击者通过精心构造数据包可以在目标主机上执行任意代码或导致目标主机蓝屏崩溃，据微软评估 TCP/IP 远程代码执行漏洞很难达成任意代码执行的效果，但是攻击者可以很容易通过分析漏洞补丁达成拒绝服务的效果。
NO.5	CVE-2021-22005	VMware vCenter Server 未授权任意文件上传漏洞	2021 年 9 月 22 日,在 VMware 官方发布的风险通告中发现 VMware vCenter Server 未授权任意文件上传漏洞（CVE-2021-22005），该漏洞是因为 VMware vCenter 的 CEIP（客户体验改善计划）分析服务中对用户提供的请求参数处理不当，攻击者利用该漏洞在未授权情况下构造恶意请求，通过 vCenter 中的 Analytics 服务 443

			端口上传恶意文件，从而造成远程代码执行漏洞。
NO.6	CVE-2021-42321	Microsoft Exchange Server 远程代码执行漏洞	Exchange Server 是一个设计完备的邮件服务器产品，提供了通常所需要的全部邮件服务功能。除了常规的 SMTP/POP 协议服务之外，它还支持 IMAP4、LDAP 和 NNTP 协议。Exchange Server 服务器有两种版本。 该远程代码执行漏洞 (CVE-2021-42321) 在经过身份验证之后，可以在 Exchange Server 上执行代码。如果 Exchange 服务器被控制，会造成非常严重的影响。 该漏洞影响版本 Exchange Server 2016、2019，因为 Exchange Server 使用广泛并且数量较多，所以此漏洞影响范围比较广泛。
NO.7	CVE-2021-42287	Microsoft Windows Active Directory 域服务权限提升漏洞	CVE-2021-42287 是由于 AD 没有对域内机器账户名做验证，导致绕过安全限制。经过远程身份验证的攻击者可以结合 CVE-2021-42278 将域内普通用户权限提升到域管理员权限。而 CVE-2021-42278 则是由于应用程序没有对 Active Directory 域服务进行适当的安全限制。结合

			CVE-2021-42287 可以导致绕过安全限制和权限提升。
NO.8	CVE-2021-1647	Windows Defender 远程代码执行漏洞	Windows Defender 曾用名 Microsoft Anti Spyware，是一个杀毒程序，运行在 Windows 系列的操作系统中。
NO.9	CVE-2021-25646	Apache Durid 远程代码执行	该漏洞的影响范围 Apache Druid < 0.20.1。产生的原因是一个 Druid 中全局性的问题，开发者在使用 Jackson 相关的标签时，出现疏漏，使得攻击者可以构造传入的 Json 串来控制一些敏感的参数进而控制服务器。
NO.10	CVE-2021-26919	Apache Druid 远程代码执行漏洞	Druid 使用 JDBC 从其它数据库读取数据，此功能是为了让受信任的用户通过适当的权限来设置查找或提交提取任务。由于 Apache Druid 默认情况下缺乏授权认证，攻击者可通过构造恶意请求执行任意代码，从而控制服务器，影响范围 Apache Druid < 0.20.2。

4.4 漏洞预警 TOP10 漏洞回顾

4.4.1 Apache Log4j2 任意代码执行漏洞

漏洞类型：远程代码执行

漏洞编号：CVE-2021-44228
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：2021-12-10
漏洞描述：

Apache Log4j2 是一款非常优秀的 Java 日志框架，是 Java 程序中最常使用的开源日志记录组件,市面上绝大多数 Java 应用都使用了该组件,在各大 Java 项目中广泛应用。该漏洞形的原因是当程序将用户输入的数据进行日志记录时，即可触发此漏洞，攻击者可通过构造恶意请求利用该漏洞实现在目标服务器上执行任意代码。

Log4j2 任意代码执行漏洞漏洞(CVE-2021-44228)产生的原因为: Apache Log4j2 某些功能存在递归解析功能，未经身份验证的攻击者通过发送特定恶意数据包，可在目标服务器上执行任意代码。该漏洞的影响版本 Apache Log4j 2.x < 2.15.0-rc2，该组件应用范围非常广泛，如：Apache Struts2、Apache Solr、Apache Druid 等开发框架及中间件中。从 Apache Log4j2 漏洞影响面查询的统计来看，影响多达 60644 个开源软件，涉及相关版本软件包更是达到了 321094 个，所以有人称这个漏洞是"核弹级",侧面说明了这个漏洞的危害。

天融信阿尔法实验室也在第一时间针对此漏洞进行了详细的分析介绍，详见下述链接：
http://blog.topsec.com.cn/%e4%bb%8e%e9%9b%b6%e5%88%b0%e4%b8%80%e5%b8%a6%e4%bd%a0%e6%b7%b1%e5%85%a5-Log4j2-jndi-rce-cve-2021-44228%e6%bc%8f%e6%b4%9e/

4.4.2 Weblogic 任意代码执行漏洞

漏洞类型：远程代码执行
漏洞编号：CVE-2021-2394
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：2021-7-21
漏洞描述：

WebLogic 是美国 Oracle 公司出品的一个 application server，确切的说是 一个基于 JAVAEE 架构的中间件,WebLogic 是用于开发、集成、部署和管理大型 分布式 Web 应用、网络应用和数据库应用的 Java 应用服务器。

2021 年 7 月 21 日，Oracle 官方发布关于 7 月份安全更新， weblogic 漏洞中编号为 CVE-2021-2394，因为影响版本多，利用难度低，被广泛的分析利用。

CVE-2021-2394:任意执行代码漏洞是一个二次反序列化漏洞， 该漏洞影响广泛，攻击者可以在未授权的情况下对 WebLogic Server 组件进行攻击。成功利用该漏洞的攻击者可以接管 WebLogic Server，该漏洞影响版本 Oracle WebLogic Server 10.3.6.0.0、12.1.3.0.0、12.2.1.3.0、12.2.1.4.0、14.1.1.0.0 版本。

4.4.3 Oracle 任意代码执行漏洞

漏洞类型：远程代码执行
漏洞编号：CVE-2021-2397

CVE-2021-2382
CVSS 3.1：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
漏洞评分：9.8、9.8
预警日期：2021-07-21
漏洞描述：

该漏洞存在于 Oracle WebLogic Server 中，Oracle WebLogic Server 是一个 Java 应用服务器，它全面实现了 J2EE 1.5 规范、最新的 Web 服务标准和最高级的互操作标准。WebLogic Server 内核以可执行、可扩展和可靠的方式提供统一的安全、事务和管理服务。

这个漏洞披漏于 7 月 21 日，之所以严重是因为该漏洞影响范围涉及到 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 等众多版本。而且攻击者可以在未授权的情况下通过 T3 或 IIOP 协议发送恶意请求，最终接管服务器。

4.4.4 Windows 的 TCP/IP 协议簇远程代码执行漏洞&拒绝服务漏洞

漏洞类型：远程代码执行&拒绝服务漏洞
漏洞编号：CVE-2021-24074
CVE-2021-24094
CVE-2021-24086
CVSS 3.1：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
漏洞评分：9.8、9.8、7.5
预警日期：*2021-02-10*
漏洞描述：

TCP/IP（Transmission Control Protocol/Internet Protocol)的简写，中文译名为传输控制协议/因特网互联协议，又叫网络通讯协议，这个协议是 Internet 最基本的协议、Internet 国际互联网络的基础，简单地说，就是由网络层的 IP 协议和传输层的 TCP 协议组成的。

该漏洞的影响范围 Windows Server 2019、2016、2012 R2、2008 R2 等版本。漏洞产生于 Windows TCP/IP 的协议簇存在远程代码执行、拒绝服务漏洞，攻击者通过精心构造数据包可以在目标主机上执行任意代码或导致目标主机蓝屏崩溃，据微软评估 TCP/IP 远程代码执行漏洞很难达成任意代码执行的效果，但是攻击者可以很容易通过分析漏洞补丁达成拒绝服务的效果。

4.4.5 VMware vCenter Server 未授权任意文件上传漏洞

漏洞类型：文件上传
漏洞编号：CVE-2021-22005
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：2021-11-26
漏洞描述：

VMware 是一家云基础架构和移动商务解决方案厂商，提供基于 VMware 的虚拟化解决方案。

2021 年 9 月 22 日,在 VMware 官方发布的风险通告中发现 VMware vCenter Server 未授权任意文件上传漏洞(CVE-2021-22005)，该漏洞是因为 VMware vCenter 的 CEIP（客户体验改善计划）分析服务中对用户提供的请求参数处理不当，在未授权情况下通过 vCenter 中的 Analytics 服务 443 端口上传恶意文件，从而造成远程代码执行漏洞，此次受到影响的版本为 VMware vCenter Server：7.0,6.7,6.5,4.x,3.x。VMware 广泛应用于世界各地，所以说在全球范围内具有较大威胁。

4.4.6 Microsoft Exchange Server 远程代码执行漏洞

漏洞类型：远程代码执行
漏洞编号：CVE-2021-42321
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：2021-11-22
漏洞描述：

Microsoft Exchange Server 是微软公司开发设计的一套电子邮件系统， 提供了通常所需要的全部邮件服务功能。除了常规的 SMTP/POP 协议服务之外，它还支持 IMAP4 、LDAP 和 NNTP 协议。Microsoft Exchange Server 服务器有两种版本。

该远程代码执行漏洞(CVE-2021-42321)在经过身份验证之后，可以在 Microsoft Exchange Server 上执行代码。漏洞影响版本 Exchange Server 2016、2019，因为 Exchange Server 使用广泛并且数量较多，所以此漏洞影响范围比较广泛。

4.4.7 Microsoft Windows Active Directory 域服务权限提升漏洞

漏洞类型：权限提升
漏洞编号：CVE-2021-42287
CVE-2021-42278
CVSS 3.1：/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
漏洞评分：8.8、8.8
预警日期：2021-12-13
漏洞描述：

CVE-2021-42287 是由于 AD 没有对域内机器账户名做验证，导致绕过安全限制。经过远程身份验证的攻击者可以结合 CVE-2021-42278 将域内普通用户权限提升到域管理员权限。而 CVE-2021-42278 则是由于应用程序没有对 Active Directory 域服务进行适当的安全限制。结合 CVE-2021-42287 可以导致绕过安全限制和权限提升。

CVE-2021-42287 漏洞影响版本：Windows Server 2004、2008、2012、2016、2019、2022 等多个版本。

CVE-2021-42278 漏洞影响版本：Windows Server 2004、2008、2012、2016、2019、

2022 等多个版本。

4.4.8 Windows Defender 远程代码执行漏洞

漏洞类型：远程代码执行
漏洞编号：CVE-2021-1647
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：2021-01-13
漏洞描述

Windows Defender 曾用名 Microsoft Anti Spyware ，是一个杀毒程序, 运行在 Windows 系列的操作系统中。

该漏洞影响范围比较广泛，Windows 10、Windows Server 2012、Windows Server 2019 等多主流版本都有受到影响，攻击者可以通过诱导受害者下载恶意构造的文件，Windows Defender 在自动扫描下载的文件时会触发漏洞，从而使攻击者控制受害者计算机。

4.4.9 Apache Durid 远程代码执行（CVE-2021-25646）

漏洞类型：远程代码执行
漏洞编号：CVE-2021-25646
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：2021-02-02
漏洞描述：

Apache Druid (incubating)是为大型数据集上的高性能片断分析（“OLAP”查询）设计的数据存储。Druid 通常用作为 GUI 分析应用程序提供动力的数据存储，或者用作需要快速聚合的高并发 API 的后端。

该漏洞的影响范围 Apache Druid < 0.20.1。攻击者可以构造传入的 Json 串来控制一些敏感的参数进而控制服务器。

4.4.10 Apache Druid 远程代码执行漏洞（CVE-2021-26919）

漏洞类型：远程代码执行
漏洞编号：CVE-2021-26919
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：2021-03-30
漏洞描述：

Apache Druid 是专为大数据集的快速切片分析（OLAP 查询）而设计的高性能分析数据库。2021 年 03 月 29 日，Apache 官方发布安全公告，公开了 Apache Druid 中的一个远程代码执行漏洞（CVE-2021-26919）

Druid 使用 JDBC 从其它数据库读取数据，此功能是为了让受信任的用户通过适当的权限来设置查找或提交提取任务。由于 Apache Druid 默认情况下缺乏授权认证，攻击者可通过构造恶意请求执行任意代码，从而控制服务器，影响范围 Apache Druid < 0.20.2。

第五章 总结

同往年相比，2021 年漏洞数量增长放缓，但并不意味着来自互联网的危害因此而降低，相反，漏洞公开的数量放缓某种程度上意味着更多的漏洞有可能选择被武器化，而选择不进行公开。

总结归纳 2021 年的高危漏洞，仍然是代码执行漏洞高居榜首，且漏洞范围涵盖操作系统、中间件、开发组件、网络协议乃至网络安全设备，如此之广的影响范围，搭配上漏洞利用成功后的高危害，如果将网络世界中不断持续的攻防对抗比作网络战争，那么代码执行漏洞就无异于战争中最先进的进攻武器。

年底披露的 Log4j2 漏洞一经发布，震动整个国内外的安全圈，甚至整个国内外的 IT 界，使用该组件的应用极为广泛，导致无数引用了该组件的系统和开源组件受到波及。Log4j2 作为开源组件中的典型代表，企业在开发的过程中，绝大多数都是用了开源组件作为自己产品的一部分，甚至在很多的开源工具中都是用了 Log4j2 作为自身的日志系统，所以这个影响的扩散范围不再是单纯的加法问题，而是一个指数级的扩散，同时 Log4j2 更为可怕的一点就是他的利用极其简单，触发点众多且分散，利用简单是在于执行远程代码的 Payload 仅仅只有一行代码，而且只需要通过正常的请求发送过去，即可触发漏洞，几乎是零利用成本，无需任何基础，攻击者都可以通过该漏洞攻击并控制一个 Java 编写的系统，由此 Log4j2 远程代码执行漏洞成为继“永恒之蓝”后又一核弹级漏洞。

随着 log4j2 远程代码执行漏洞的扩散，供应链安全再一次被摆放到了聚光灯下，这次的事件让厂商们意识到供应链的安全有多么脆弱，在整个供应链中，很多供应商在开发程序的时候都会选择引入第三方库，有的项目甚至会引入上百个三方库之多，而这些三方库只要有一个存在安全问题，那么厂商就会暴露在网络安全威胁之下，可能会因此导致企业重要系统被植入勒索病毒、服务器崩溃、用户数据泄露、企业员工个人信息泄露，甚至是企业商业机密的泄露，从而引发无穷的隐患。

随着安全的不断发展，从业人员数量日益增加，与此同时安全研究人员的漏洞挖掘能力也在不断增强，辅以不断更新迭代的漏洞挖掘工具，更多的漏洞也将会被不断披露。面临激增的漏洞数量，如果企业难以解决这些漏洞所带来的问题，企业安全则将受到严重的损害。例如 2017 年 4 月 14 日 Shadow Brokers 组织公布的永恒之蓝，在接下来的一段时间中，勒索病毒借由此漏洞进行快速传播，全球众多企业因此遭受勒索病毒侵害，最终无奈向其支付赎金。

为了从根源上避免安全事件的发生，就应该从源头上减少漏洞的产生。这就要求开发人员在掌握编程能力的同时，还应具备安全开发意识，熟悉 CWE TOP25（MITRE 公布的前 25 个最危险软件安全缺陷知识库）漏洞的成因及危害。与此同时，应将安全性测试环节添加到软件的开发过程中，使得项目具备 DevSecOps 能力，至少应在软件开发过程中增加代码审计工程师或代码审计工具对代码进行审计的步骤。但是漏洞并不会被彻底消灭，而所谓的安全性不是指“安全”或“不安全”，而是取决于对安全事件的响应速度。只有提高漏洞管理效率，才是最有效的安全处理法则。

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。天融信将充分发挥自身优势，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。