RELIABLE NETWORK
SAFE WORLD
TOPSEC

2020 年网络安全漏洞趋势及漏洞统计分析报告

天融信阿尔法实验室

目录

一、前言

随着网络和信息化的飞速发展，社交网络、移动互联网、物联网等新技术不断涌现，网络安全问题逐渐凸显并成为了影响经济、政治、社会等诸多领域持续发展进步的关键因素。

网络安全漏洞主要指信息技术、产品及系统在需求、设计、实现、配置、维护和使用等过程中所产生的安全缺陷，这些缺陷一经恶意利用就会对信息产品或系统造成安全损害，影响正常服务运行并危害网络安全。

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《2020 年网络安全漏洞趋势及漏洞统计分析报告》，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 2020 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，2019 年共披露漏洞 16050 枚，2020 年共披露漏洞 19930 枚，同比增长 24.17%。2020 年高危漏洞类型分布相对集中，表现为远程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 2020 年度高危漏洞预警情况概述，依据漏洞影响范围、影响对象、产生威胁等关键因素，我们筛选出 TOP10 重点漏洞。2020 年度重点漏洞含 Netlogon 权限提升、SMBv3 远程代码执行、Weblogic IIOP 远程代码执行、Exchange Server 远程代码执行、Windows DNS Server 远程代码执行及 Apache Struts2 远程代码执行漏洞等。安全漏洞数量整体呈上升趋势，其中高威胁漏洞数量和占比均有所增加，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。

二、2020 年漏洞趋势

1. CNVD 漏洞库 2020 年漏洞统计概况

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 2020 年披露的漏洞进行了全方位的统计分析,具体统计情况如下:

2019 年一共披露漏洞 16050 枚，2020 年一共披露漏洞 19930 枚。同比增长 24.17%。其中高危漏洞 6903 枚，同比增长 42.36%。中危漏洞 10616 枚，同比增长 10.91%。低危漏洞 2411 枚，同比增长 48%，各级别漏洞数量均处于近 10 年新高。

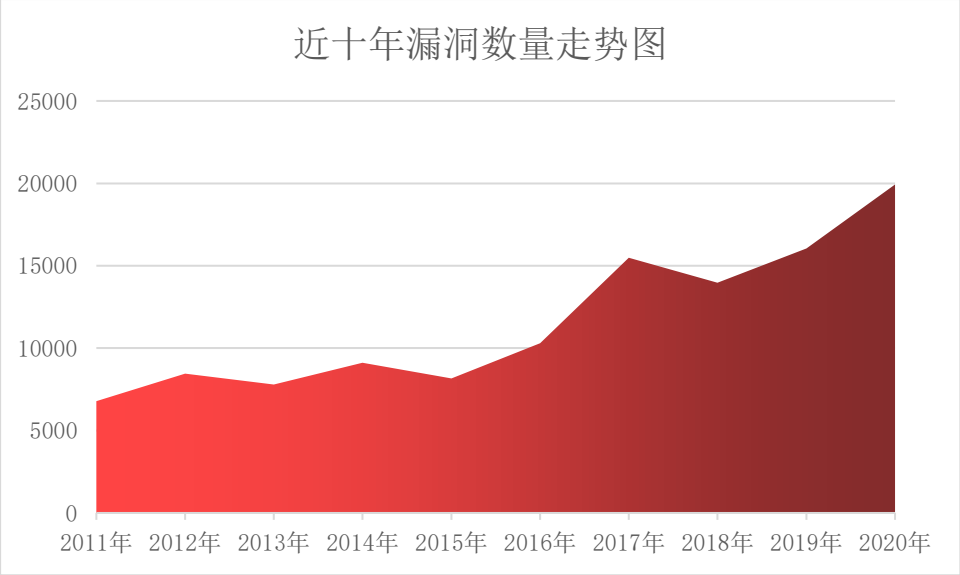

图 1 近十年漏洞数量走势图(数据来自于 CNVD)

1) 漏洞威胁等级统计

根据 2020 年 1-12 月漏洞引发威胁严重程度统计，其中低危漏洞 10.6%，中危漏洞 52.6%，高危漏洞 36.8%。

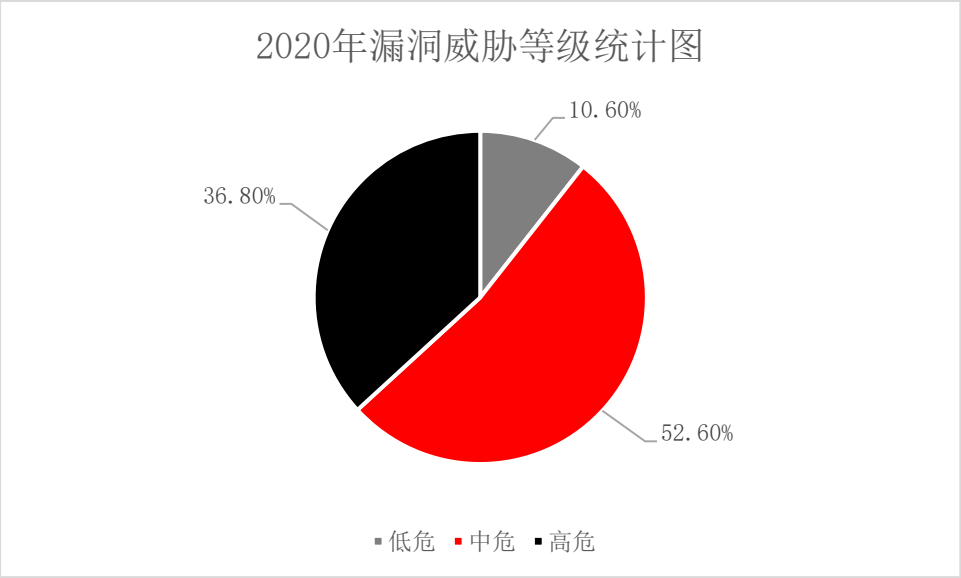

图 2 2020 年收录漏洞按威胁级别统计(数据来自于 CNVD)

2) 漏洞利用攻击位置统计

根据 2020 年 1-12 月漏洞引发威胁统计，其中远程攻击占比约为 80.2%，本地攻击约占 17.9%，其他攻击为 1.8%。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。

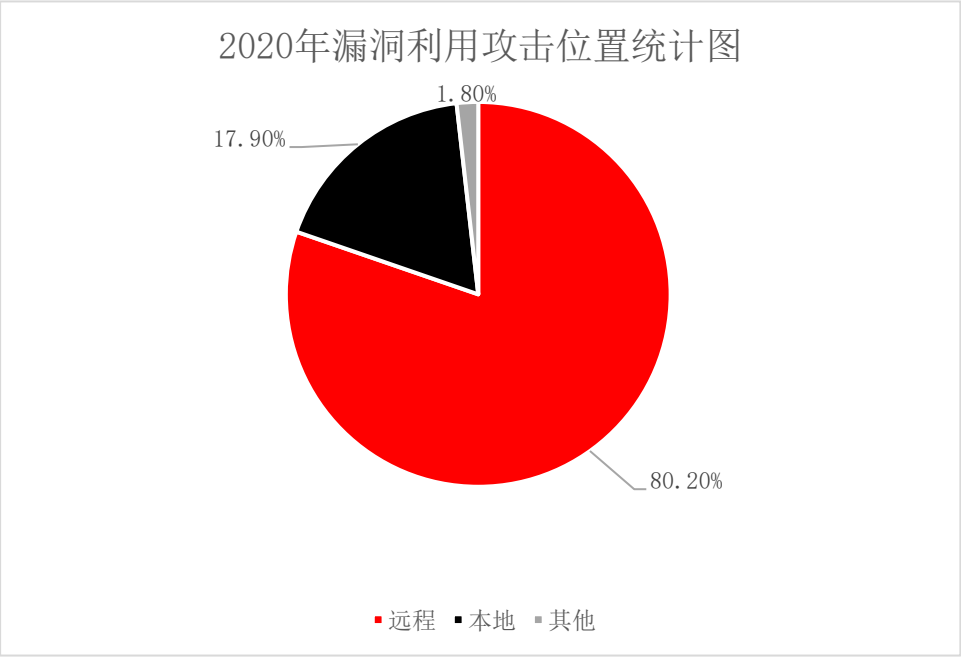

图 3 2020 年收录漏洞按利用的攻击位置统计（数据来自于 CNVD）

3） 漏洞影响对象类型统计

根据 2020 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。其中应用程序漏洞 48%，WEB 应用漏洞 27.7%，操作系统漏洞 10.3%，网络设备漏洞 6.8%，智能设备漏洞 2.1%，区块链公链漏洞 1.9%，安全产品漏洞 2%，数据库漏洞 1.3%。

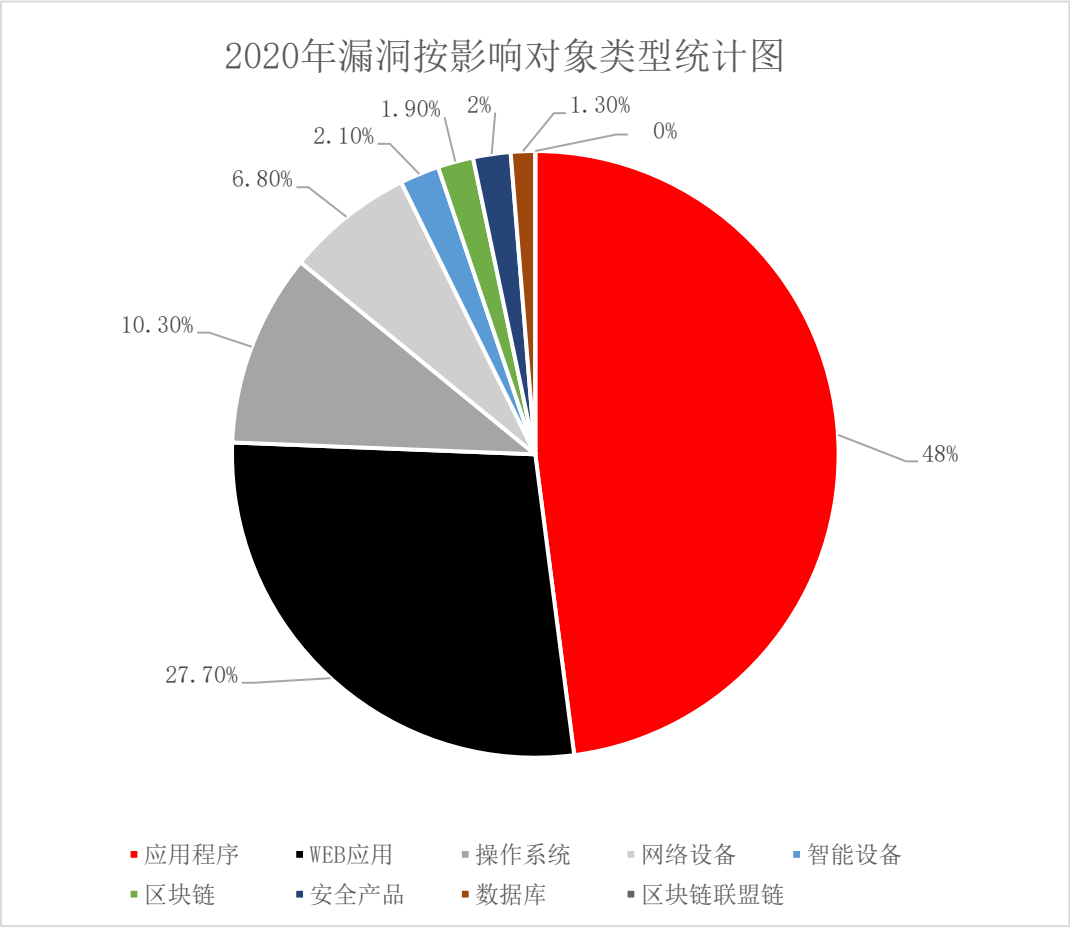

图 4 2020 年漏洞按影响对象类型统计（数据来自于 CNVD）

4） 漏洞产生原因统计

根据 2020 年 1-12 月漏洞产生原因的统计，设计错误导致的漏洞占比 65.4%屈居首位，紧跟其后的是输入验证错误导致的漏洞 25.4%位居第二，接着是边界

条件错误导致的漏洞占比 5.3%位居第三。后面的意外情况处理错误，访问验证错误，配置错误，竞争条件，环境错误，其他错误。分别为 0.1%、1.4%、0%、0.2%、0%、2.1%。

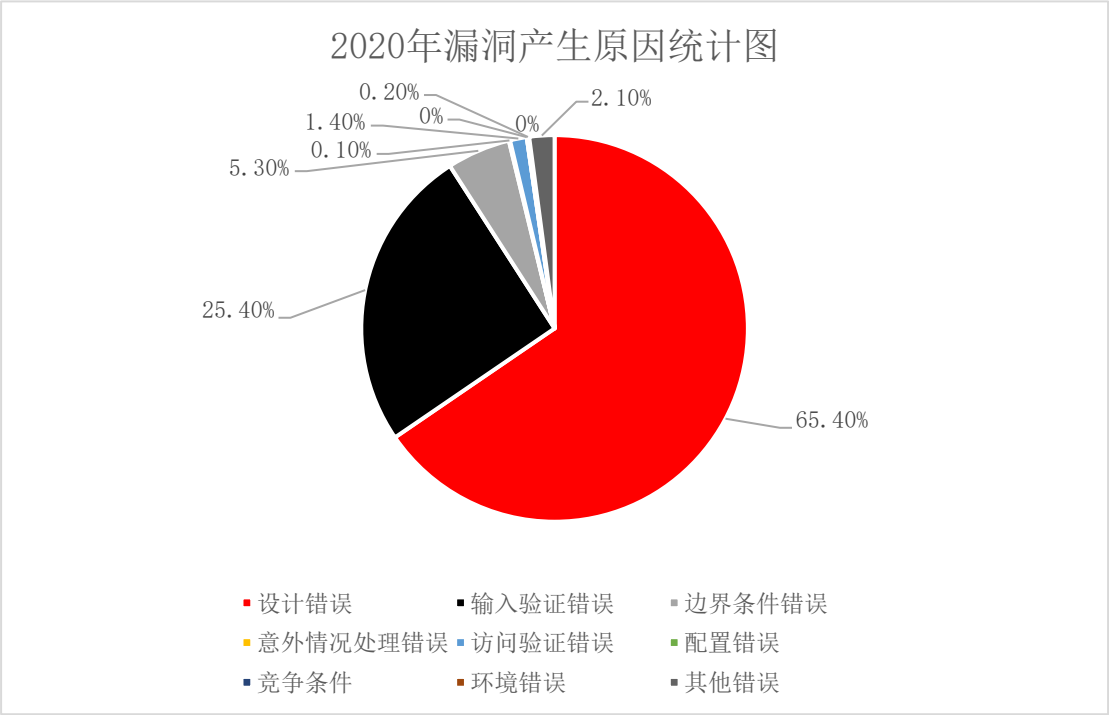

图 5 2020 年漏洞按产生原因统计（数据来自于 CNVD）

5） 漏洞引发威胁统计

根据 2020 年 1-12 月漏洞引发威胁统计，未授权信息泄露占比 28.3%屈居首位，紧跟其后的是管理员访问权限获取漏洞 24.6%位居第二，接着是拒绝服务占比 16.2%位居第三。后面的普通用户访问权限获取，未授权信息修改，其它，未知。分别为 5%，12.5%，11.7%，1.7%。

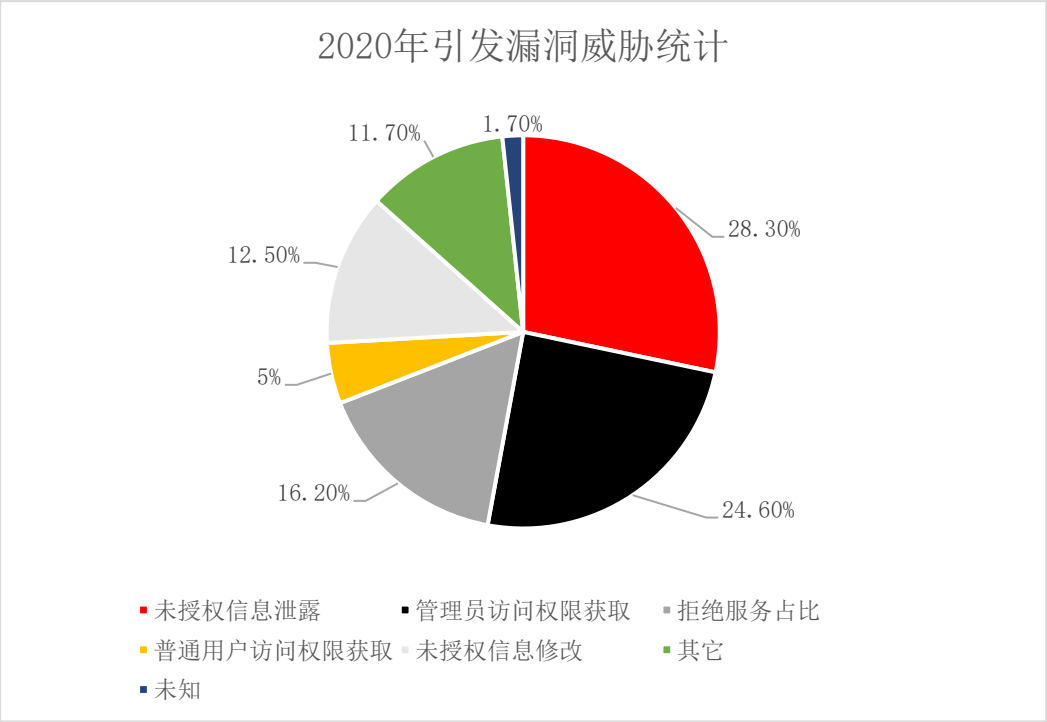

图 6 2020 年漏洞按引发威胁统计（数据来自于 CNVD）

2. 2020 年 CVE TOP100 漏洞统计概况

通过对 CVE 在 2020 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三星、高通及 Oracle。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 44%，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 7 月份共披露高危漏洞 17 个，位居全年第一。在 TOP100 漏洞中大约有 16%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 79%，本地利用的漏洞约占 21%，来自互联网的漏洞依旧是主要的攻击手段。在 TOP100 高危漏洞中，远程代码执行类型的漏洞共占比 71%。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。

具体统计分析结果如下：

1） 漏洞影响厂商分布情况

根据 2020 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，前三名分别是三星、QUALCOMM 及 Oracle。其中三星厂商的产品占比达到 53%，QUALCOMM 的产品占到 17%，Oracle 的产品共占 7%。

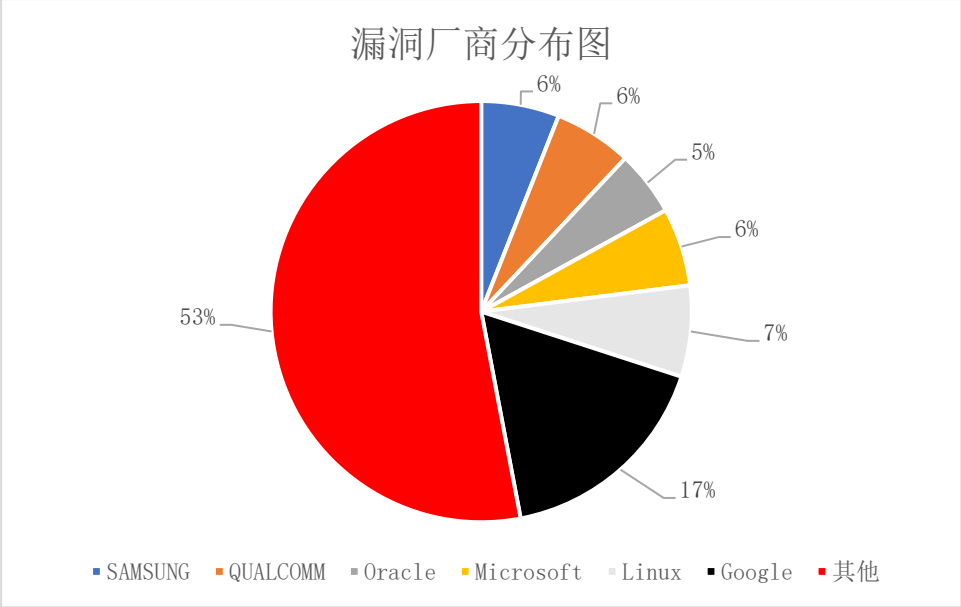

图 7 漏洞厂商分布图（数据来自于 CVE）

2） 高危漏洞披露时间趋势图

根据 2020 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 2020 年全年中，7 月份披露 17 个 TOP100 漏洞占比 17%位居第一，4 月与 3 月份分别披露 13、12 个漏洞位居第二与第三，而 2 月份未有 TOP100 漏洞被披露。

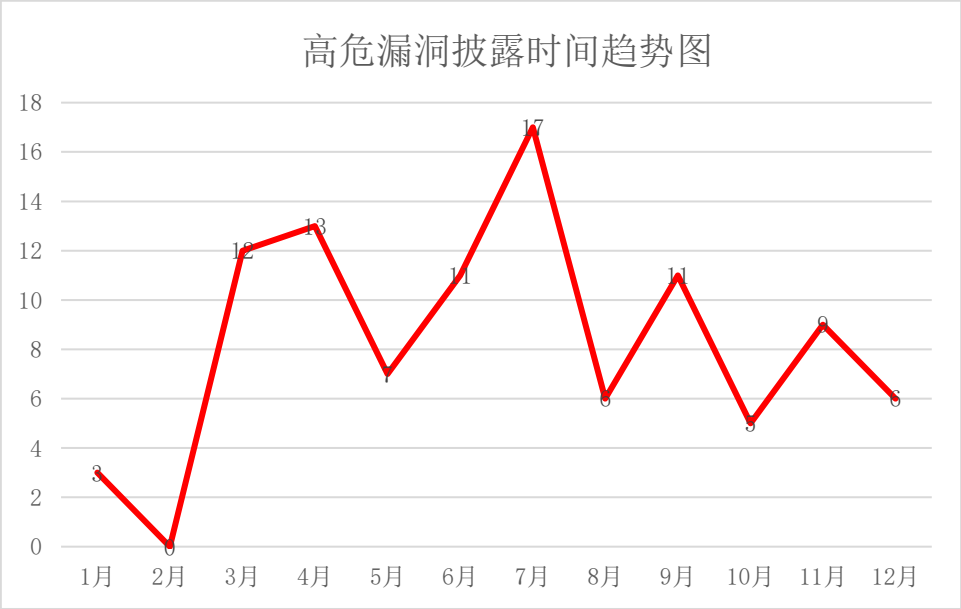

图 8 高危漏洞披露时间趋势图（数据来自于 CVE）

3） 攻击途径概况

根据 2020 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 79%，本地攻击约占 21%。由此可见来自公网的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。

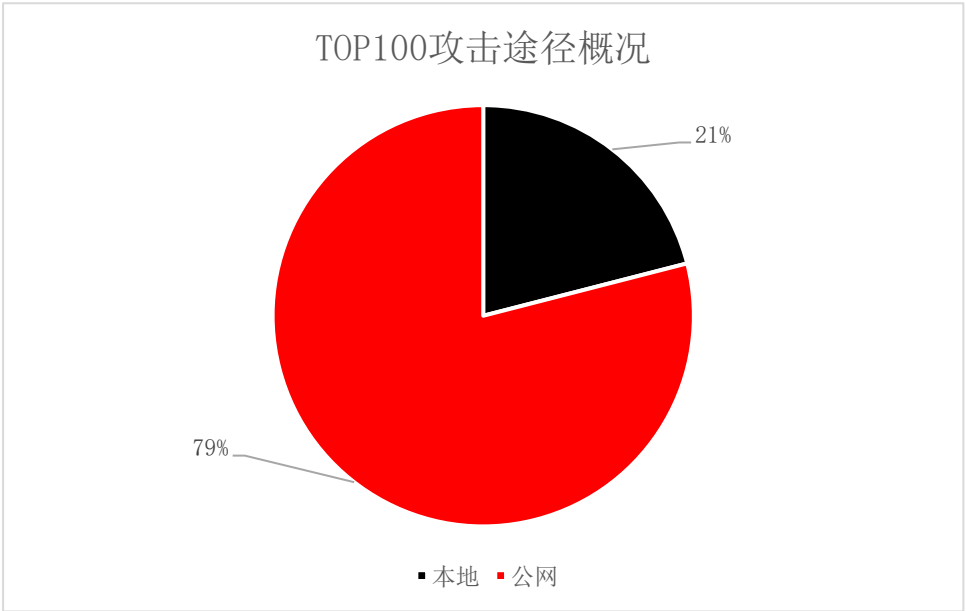

图 9 TOP100 攻击途径概况（数据来自于 CVE）

4） 漏洞影响平台分类

根据 2020 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 44%，移动端平台漏洞 32%，硬件设备平台漏洞 9%，跨平台漏洞 7%，其他漏洞 8%。

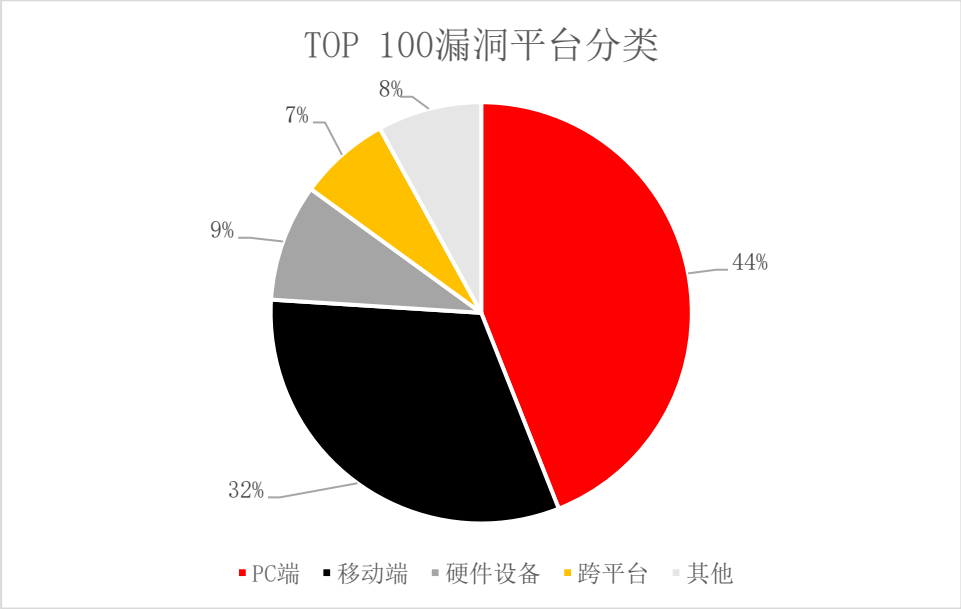

图 10 TOP100 漏洞平台分类（数据来自于 CVE）

5） 漏洞类型统计概况

根据 2020 年 1-12 月 CVE 披露漏洞危害程度前 100 例类型进行统计，其中远程代码执行漏洞占比最多，以 71%位居首位，而权限提升、内存破坏、命令执行、以及其他漏洞分别占比 10%、7%、5%、4%、3%。

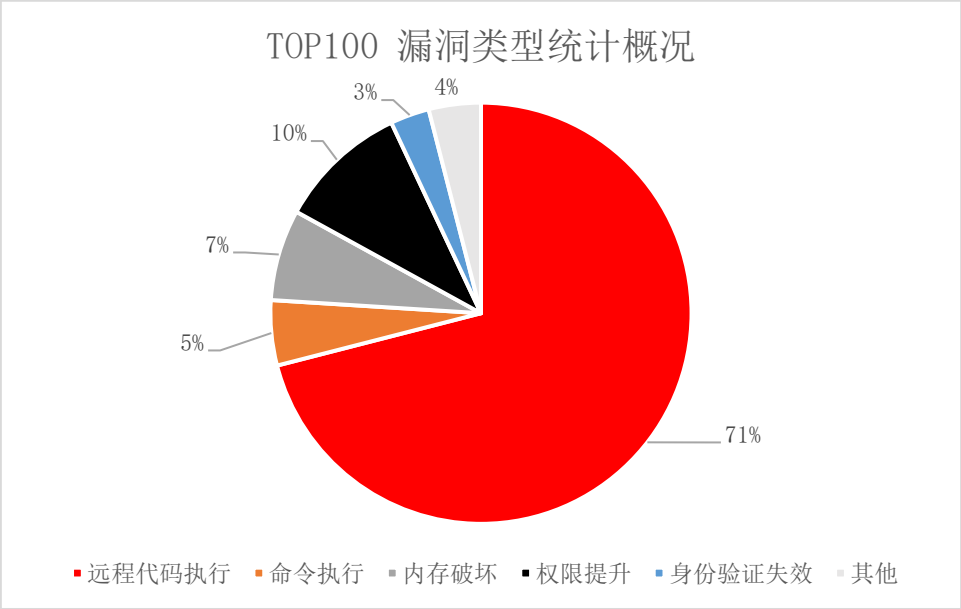

图 11 TOP100 漏洞类型统计概况（数据来自于 CVE）

6） TOP100 POC 公开情况统计

根据 2020 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 45%，公开 POC 的仅有 16%，而有 39%的漏洞未有明确的 POC 公开情况。

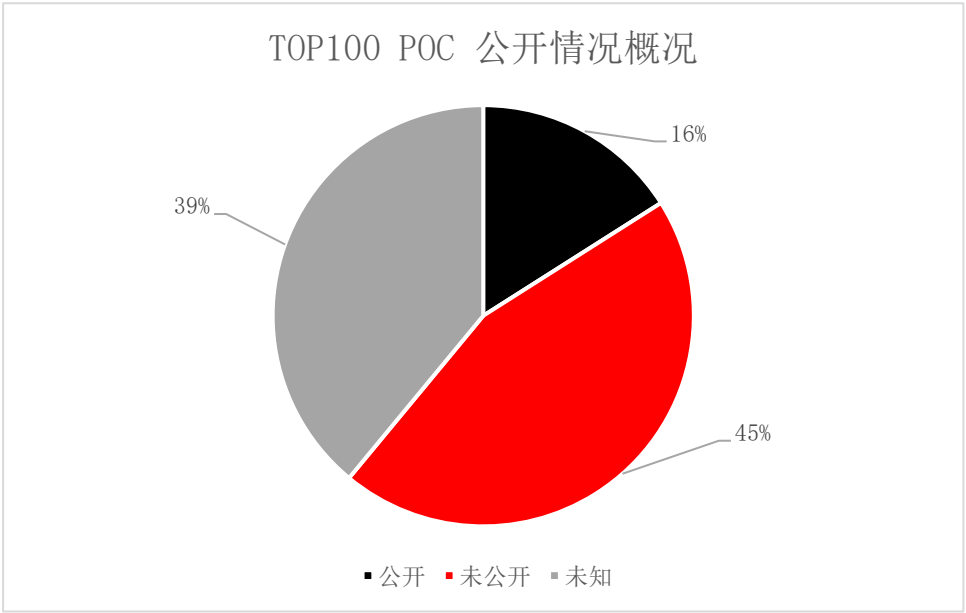

图 12 TOP100 POC 公开情况概况（数据来自于 CVE）

三、漏洞预警统计概况

天融信阿尔法实验室在 2020 年共发布高危漏洞风险提示通告 61 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。2020 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。Weblogic、WebSphere、SMB 协议、Openssl 等关键基础设施漏洞也是受关注度较高的方向。

2020 年预警的漏洞中，代码执行类漏洞占比最高，达到 58%。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：

1. 漏洞厂商情况

在 2020 年内发布的 61 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 23%，针对 Apache 厂商的漏洞预警为 8 次，占比约 13%位居第二名，而针对 Oracle 与 VMware 厂商的各 5 次，并列位居第三名。

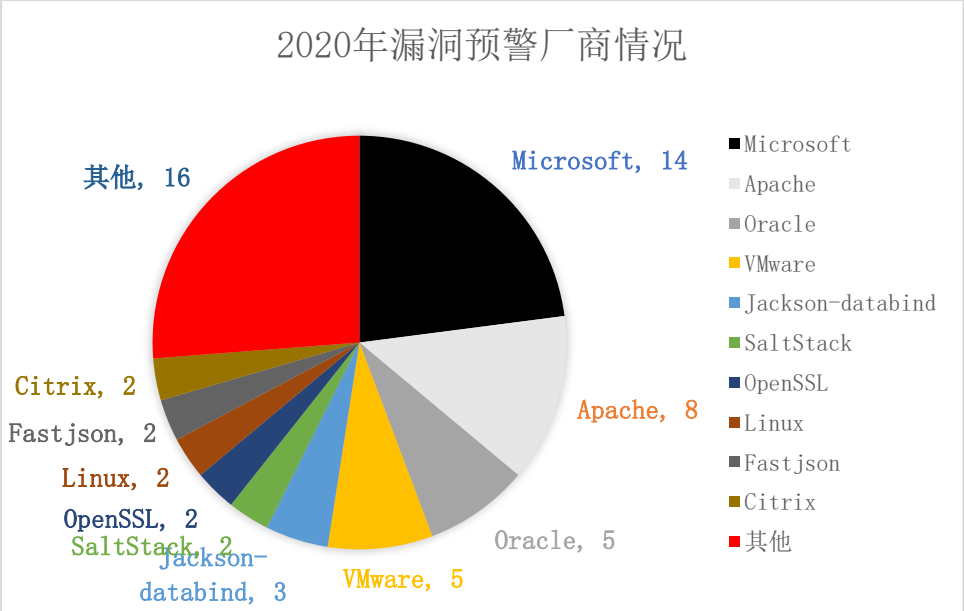

图 13 2020 年漏洞预警厂商情况

2. 漏洞威胁情况

在 2020 年发布的 61 条漏洞通告中，所通告的漏洞可分为 8 大类，分别是代码执行漏洞、拒绝服务漏洞、权限绕过漏洞、文件操作类漏洞、命令执行漏洞、虚拟机逃逸漏洞、注入漏洞以及其他漏洞，其中代码执行漏洞占 58%位于首位，拒绝服务、权限绕过以及其他漏洞分别占比 8%共同位于第二位，虚拟机逃逸与注入类漏洞分别占比 3%位于末位。

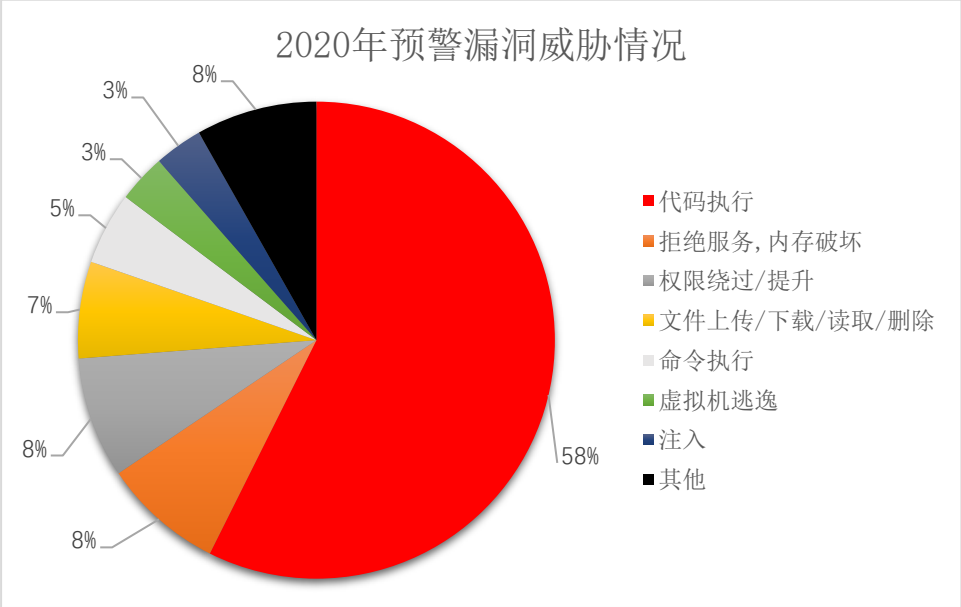

图 14 2020 年预警漏洞威胁情况

3. 年度 TOP10 漏洞

针对 2020 年所爆发的高危漏洞，天融信根据漏洞危害程度及影响范围，归纳筛选出 2020 年 10 个重点安全漏洞，详情如下：

漏洞编号	标题	概述
CVE-2020-1472	Microsoft NetLogon 远程权限提升漏洞	漏洞影响版本广泛，攻击者利用此漏洞，无须身份验证即可获取域控制器的管理员权限并在设备上运行经特殊设计的应用程序，可对受害者资产造成极大的破坏。

CVE-2020-0796	Microsoft SMBv3 协议远程代码执行漏洞	本次漏洞主要影响了 Windows 10 以及 Windows Server 下的多个版本，其影响面及其广大，推测可能在未来会成为恶意软件和攻击者广泛利用的漏洞。
CVE-2020-17530	Apache Struts2 S2-061 远程代码执行漏洞	Apache Struts2 作为世界上最流行的 Java Web 服务器框架之一被各大公司采用，该漏洞影响了 Apache Struts 2.0.0 - 2.5.25，影响面极其广泛。
CVE-2020-2551	Weblogic IIOP 远程代码执行漏洞	攻击者可以通过 IIOP 协议远程访问 Weblogic Server 服务器上的远程接口，传入恶意数据，从而获取服务器权限并在未授权情况下远程执行任意代码，由于 IIOP 协议以 Java 接口的形式对远程对象进行访问且默认启用，而 Weblogic 作为 Oracle 的主要产品之一在全世界范围内被大量使用，该漏洞在全球范围内造成了极大的影响。
CVE-2020-14882	Weblogic Console HTTP 协议代码执行漏洞	WebLogic 远程代码执行漏洞 CVE-2020-14882 和 CVE-2020-14883 两个高危漏洞 POC 已经公开,未经身份验证的攻击者可以通过构造恶意 HTTP 请求利用该漏洞,成功利用此漏洞可能接管 Oracle WebLogic Server。 该漏洞影响了 Oracle Weblogic Server 10.3.6、12.1.3、12.2.1.3、12.2.1.4、14.1.1.0 版本，影响极为广泛。
CVE-2020-0688	Microsoft Exchange	Exchange Server 是微软的一款消息与协作系统，在全球有着庞大的使用量，该漏洞

	Server 远程代码执行漏洞	所带来的影响面及为广泛。
CVE-2020-1350	Windows DNS Server 远程代码执行漏洞	微软官方认为这是一个可蠕虫攻击的漏洞，可以在易受攻击的计算机之间传播，而不需要用户交互。该漏洞影响程度较为严重，建议所有运行 DNS 服务器的用户尽快更新安全补丁。
CVE-2020-0618	SQL Server 远程代码执行漏洞	本次漏洞影响了 Microsoft SQL Server 2012、2014 以及 2016 版本，SQL Server 在国内外拥有众多用户，漏洞具有一定影响。
CVE-2020-5902	F5 BIG-IP TMUI 远程代码执行漏洞	攻击者利用该漏洞，通过向 TMUI 发送恶意攻击请求，从而执行任意系统命令、创建或删除文件、禁用服务，以及执行任意 Java 代码，最终完全获取系统权限。
CVE-2020-1948	Apache Dubbo 远程代码执行漏洞	Apache Dubbo 作为一个优秀的服务框架被广泛使用，该漏洞影响了 Dubbo 2.7.0 - 2.7.6、2.6.0 - 2.6.7、2.5.x 版本，具有较大的威胁。

四、漏洞预警 TOP10 漏洞回顾

1. Microsoft NetLogon 远程权限提升漏洞

1）漏洞描述

该漏洞是 Windows Server 在实现登录验证的 AES-CFB8 加密算法初始化 IV 时不恰当的使用随机数导致，在初始化 IV 时有 1/256 的概率使得 IV 为全 0，导致加密得到的密文全 0，最终导致身份验证被绕过。未经身份验证的远程攻击者利用此漏洞无需身份验证即可获取域控制器的管理员权限。

该漏洞影响版本广泛，Windows Server 2008、2012、2016、2019 等多个 Windows Server 版本受到此漏洞影响。攻击者利用此漏洞，无须身份验证即可获取域控制器的管理员权限并在设备上运行经特殊设计的应用程序。成功的利用该漏洞，可能会对受害者资产造成极大的破坏。

2. Microsoft SMBv3 协议远程代码执行漏洞

1）漏洞描述

本次漏洞存在于微软 SMBv3.0 协议中，该漏洞是由 SMBv3 处理恶意压缩数据包时进入错误流程造成的。未经身份验证的攻击者可以通过利用该漏洞，向存在漏洞的受害主机的 SMBv3 服务发送特殊构造的数据包即可远程执行任意代码。

本次漏洞主要影响了 Windows 10 以及 Windows Server 下的多个版本，其影响面及其广大，推测可能在未来会成为恶意软件和攻击者广泛利用的漏洞。

天融信阿尔法实验室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/cve-2020-0796-lpe-%e6%b7%b1%e5%ba%a6%e5%88%86%e6%9e%90/

3. Apache Struts2 S2-061 远程代码执行漏洞

1）漏洞描述

Apache Struts 2 最初被称为 WebWork 2，它是一个简洁的、可扩展的框架，可用于创建企业级 Java web 应用程序。设计这个框架是为了从构建、部署、到应用程序维护方面来简化整个开发周期。

Apache Struts 于 2020 年 12 月 08 日披露 S2-061 Struts 远程代码执行漏洞（CVE-2020-17530），在使用某些 tag 等情况下可能存在 OGNL 表达式注入漏洞，从而造成远程代码执行，风险极大。

该漏洞主要影响了 Apache Struts 2.0.0 - 2.5.25，而 Apache Struts2 作为世界上最流行的 Java Web 服务器框架之一被各大公司采用，因此该漏洞影响面极其广泛。

2）数据分析

天融信安全云服务运营中心通过风险探知系统对我国境内部署 Apache Struts2 的服务器进行统计，结果显示我国境内的 Apache Struts2 的服务器约有 80672 台。按区域统计来看，排名前三的省份是北京市 17339 台，浙江省 32506 台，广东省 14266 台。

下图为中国范围内使用 Apache Struts2 的服务器分布情况：

图 15 国内分布图

下图为使用 Apache Struts2 的服务器的国内运营商排名：

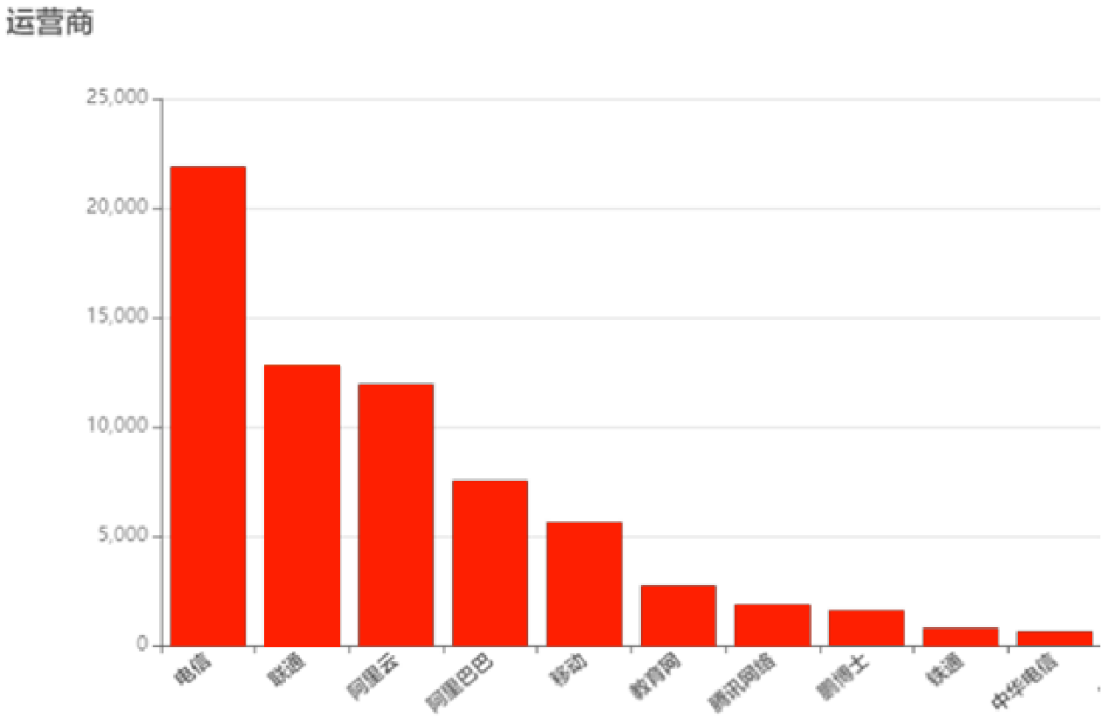

图 16 国内运营商排名前十

下图为使用 Apache Struts2 的服务器的端口排名：

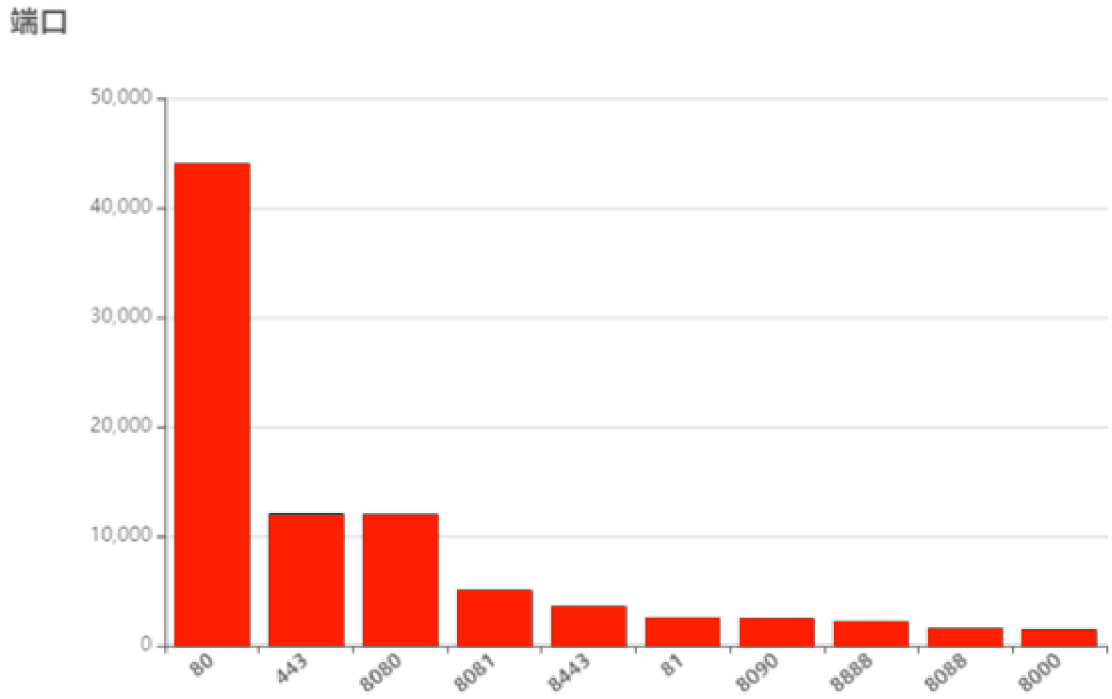

图 17 国内端口统计排名前十

下图为使用 Apache Struts2 的服务器的国内操作系统排名：

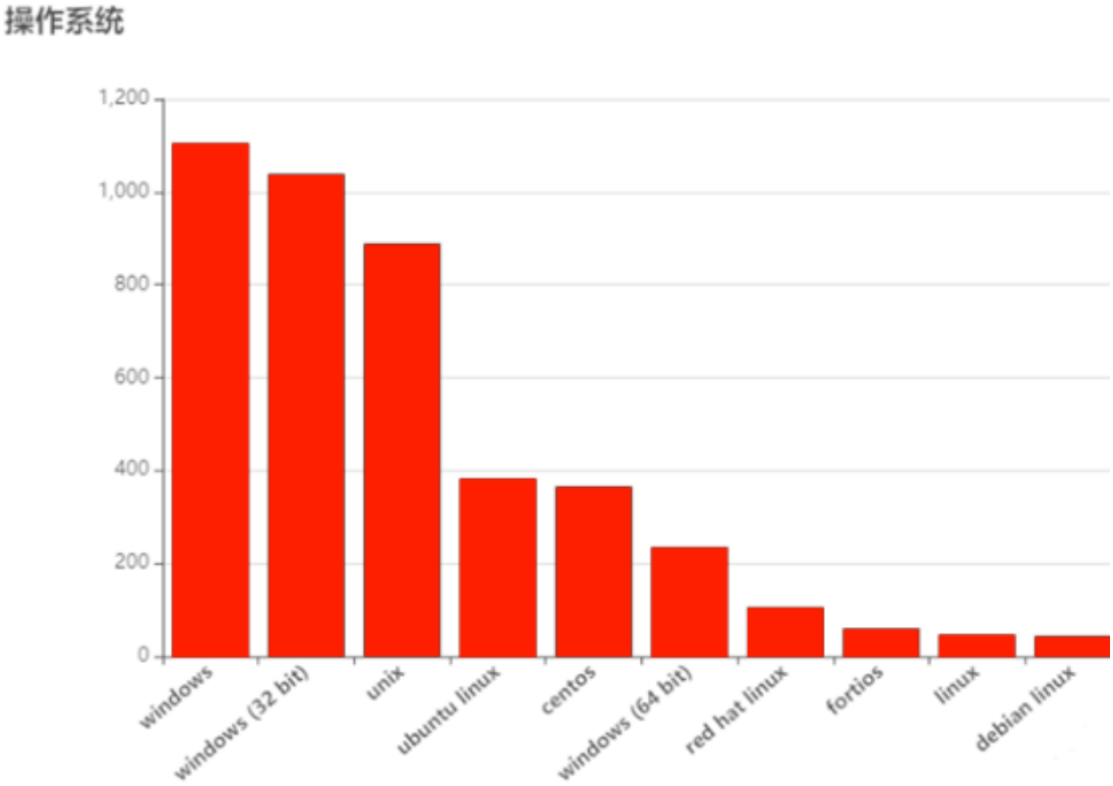

图 18 国内操作系统统计排名前十

4. Weblogic IIOP 远程代码执行漏洞

1）漏洞描述

CVE-2020-2551 存在于 Weblogic WLS 组件 IIOP 协议。互联网内部对象请求代理协议(IIOP)是一个实现互操作性的协议，它使得由不同语言编写的分布式程序在因特网中可以实现彼此的交流沟通。它是行业战略性标准，也即公用对象请求代理程序结构(Common Object Request Broker Architecture，CORBA)中至关重要的一个部分。

该漏洞影响了 Oracle WebLogic Server10-12 版本，攻击者可以通过 IIOP 协议远程访问 Weblogic Server 服务器上的远程接口，传入恶意数据，从而获取服务器权限并在未授权情况下远程执行任意代码，由于 IIOP 协议以 Java 接口的形式对远程对象进行访问且默认启用，而 Weblogic 作为 Oracle 的主要产品之一在全世界范围内被大量使用，该漏洞在全球范围内造成了极大的影响。

天融信阿尔法实验室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/weblogic-cve-2020-2551%e6%bc%8f%e6%b4%9e%e5%88%86%e6%9e%90/

2）数据分析

天融信安全云服务运营中心通过风险探知系统对世界范围内部署 Weblogic 的服务器进行统计，结果显示 Weblogic 服务器约有 7987 台。按统计来看，排名前五的国家是中国、法国、美国、越南、印度。

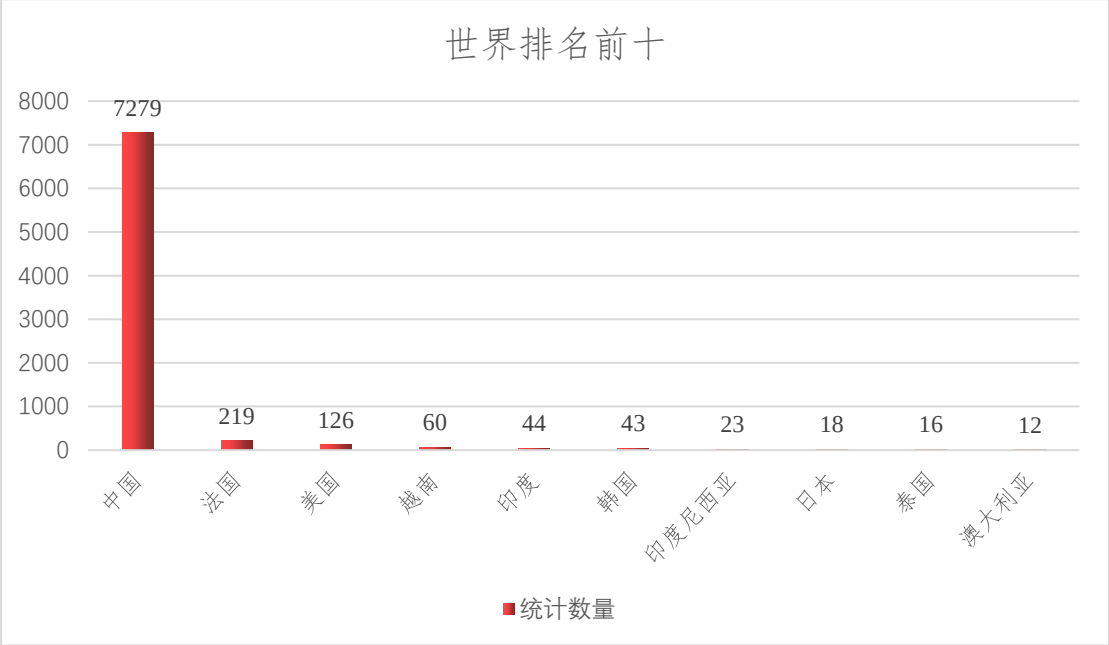

图 19 世界排名前十

天融信安全云服务运营中心通过风险探知系统对我国境内部署 Weblogic 的服务器进行统计，结果显示我国境内的 Weblogic 的服务器约有 7262 台。按区域统计来看，排名前五的省份或地区为北京市、广东省、上海市、浙江省、江苏省。

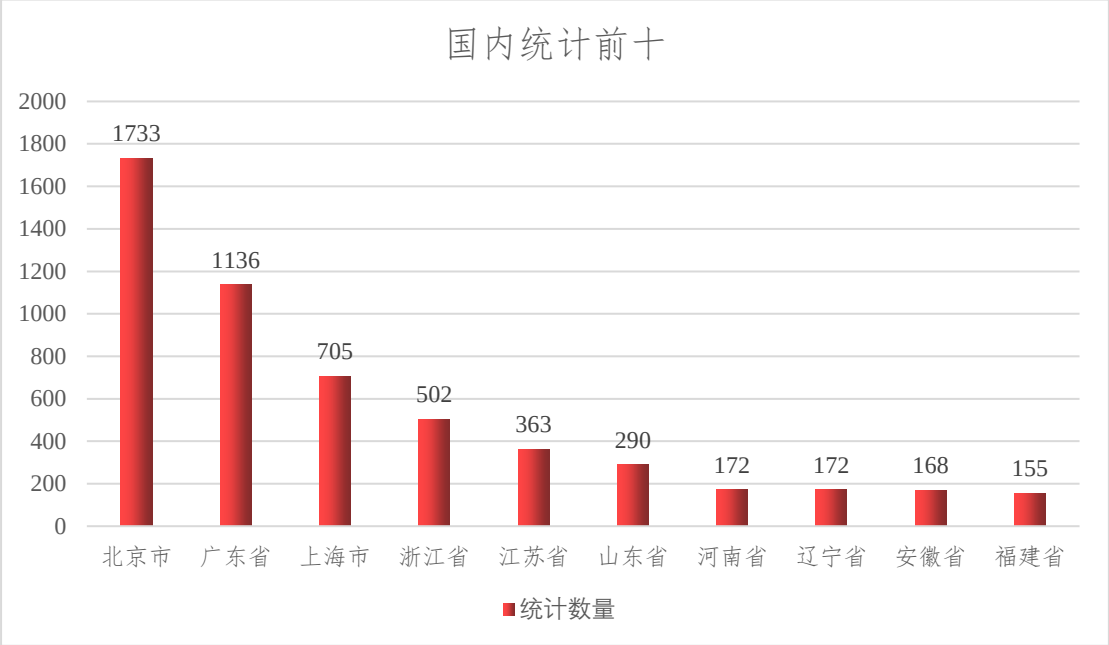

图 20 国内统计前十

按运营商统计来看，排名前五的运营商分别为电信、联通、移动、阿里云、教育网。

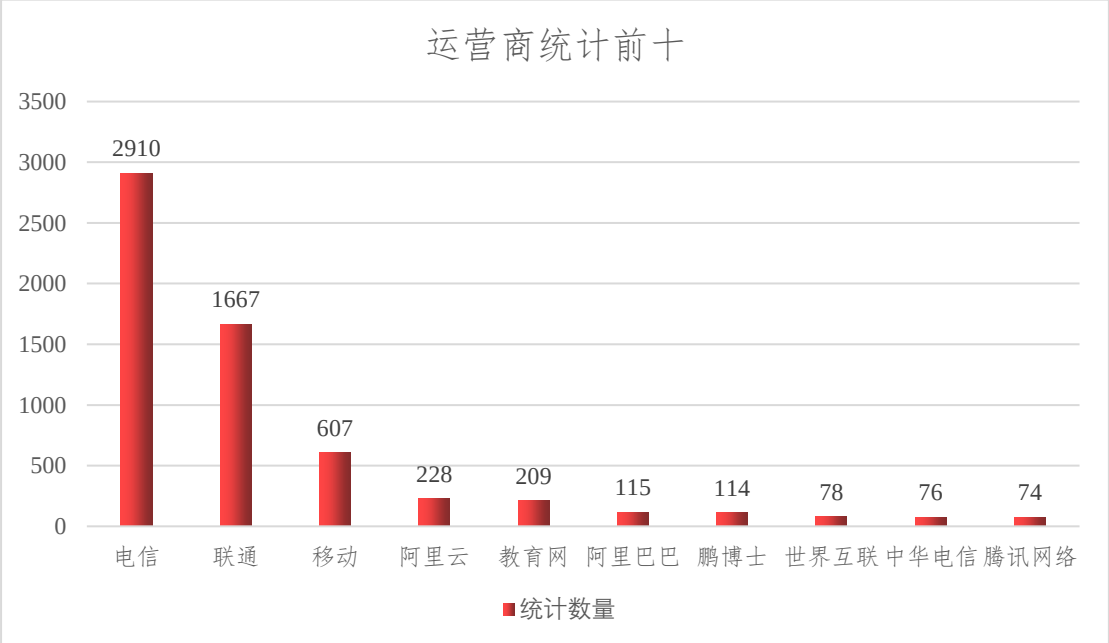

图 21 运营商统计前十

按端口统计数量来看，排名前五的端口分别为 80、443、8001、7001、8080。

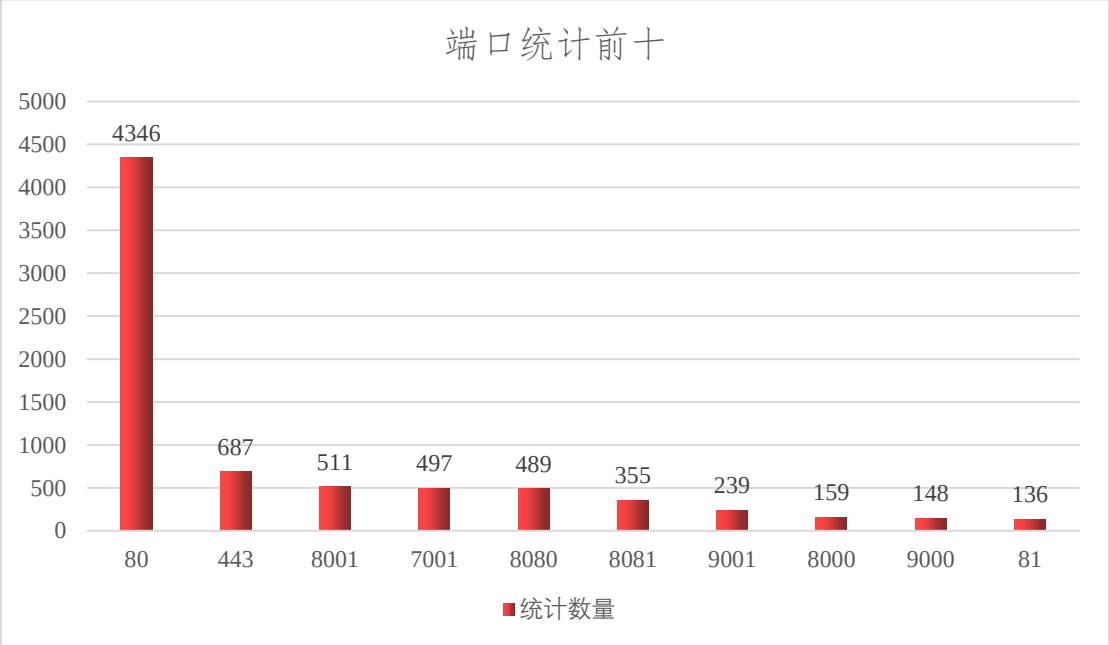

图 22 端口统计前十

5. Weblogic Console HTTP 协议代码执行漏洞

1）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。

WebLogic 远程代码执行漏洞 CVE-2020-14882 和 CVE-2020-14883 两个高危漏洞 POC 已经公开,未经身份验证的攻击者可以通过构造恶意 HTTP 请求利用该漏洞,成功利用此漏洞可能接管 Oracle WebLogic Server。

Weblogic 作为 Oracle 的主要产品之一，是商业市场上主要的 Java（J2EE）应用服务器软件(application server)之一,是世界上第一个成功商业化的 J2EE 应用服务器被世界,在全世界范围内被大量使用,该漏洞影响了 Oracle Weblogic Server 10.3.6、12.1.3、12.2.1.3、12.2.1.4、14.1.1.0 版本，因此在全世界范围造成了极大的影响。

6. Microsoft Exchange Server 远程代码执行漏洞

1）漏洞描述

此漏洞是由于 Microsoft Exchange 控制面板（ECP）组件中使用静态密钥造成的。根据 POC 来看，本次利用需要攻击者拥有一个邮箱账号并使用该账号登录服务器，在登陆过程中获取凭证，进而通过获取到的凭证构造出恶意数据，最终向存在漏洞的 ECP 组件发送包含恶意数据的请求进行攻击。执行此攻击无需用户交互，并且会以系统级别权限执行，从而完全控制 Exchange 服务器。

该漏洞影响了 Microsoft Exchange Server 2010 、2013、2016、2019 版本。Exchange Server 是微软的一款消息与协作系统，在全球有着庞大的使用量，该漏洞所带来的影响面及为广泛。

2）数据分析

天融信安全云服务运营中心通过风险探知系统对我国境内部署的 Microsoft Exchange 服务器进行抽样统计，结果显示我国境内暴露在互联网中的 Microsoft Exchange 服务器有 1.2 万余台，这些服务器开放最多的端口是 25 和 110，其次是 587、143 和 995。按区域统计来看，排名前三的省份是广东省 2948 台，上海市 2395 台，香港特别行政区 2109 台。

图 23 全国区域分布

下图为中国范围内部署的 Microsoft Exchange 服务器数量排名前五省份或地区：

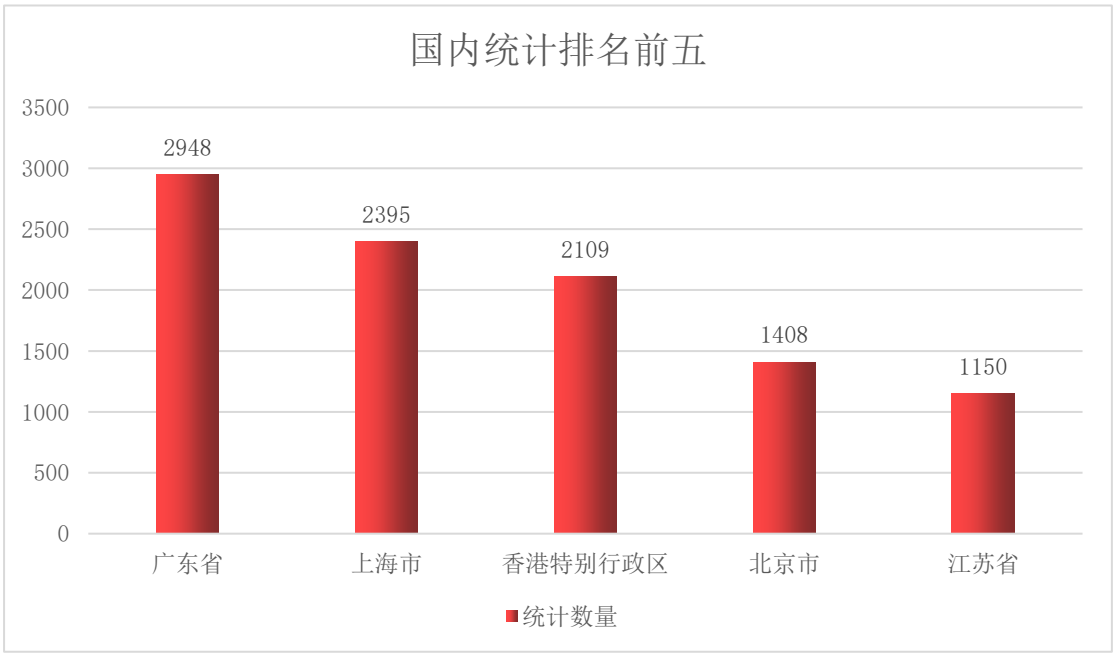

图 24 全国排名前五

7. Windows DNS Server 远程代码执行漏洞

1）漏洞描述

此漏洞源于 Microsoft DNS Server 实现中的缺陷。利用此漏洞，未经身份验证的攻击者通过向 Microsoft DNS Server 发送恶意请求，可执行任意代码。

微软官方认为这是一个可蠕虫攻击的漏洞，可以在易受攻击的计算机之间传播，而不需要用户交互。该漏洞影响程度较为严重，建议所有运行 DNS 服务器的用户尽快更新安全补丁。此外该漏洞仅影响 Microsoft 的 Windows DNS Server 实现，不会影响 Windows DNS 客户端。

2）数据分析

天融信安全云服务运营中心通过风险探知系统对世界范围内部署 Microsoft DNS 的服务器进行统计，结果显示 Microsoft DNS 服务器约有 230338 台。按统计来看，排名前五的国家是美国、中国、土耳其、英国、德国。

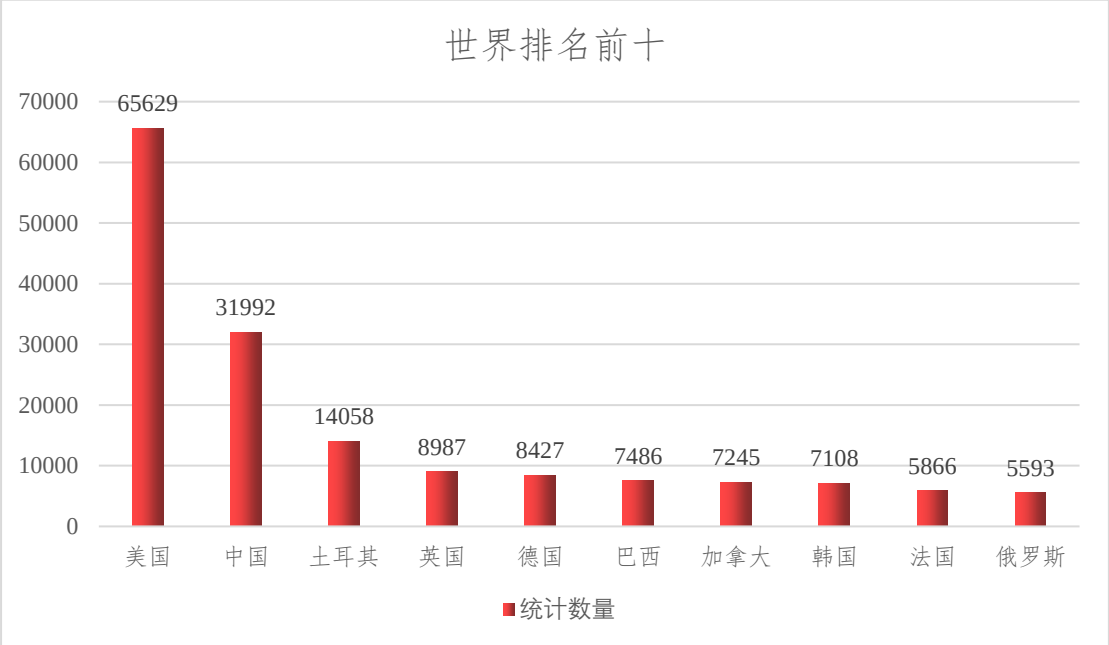

图 25 世界排名前十

天融信安全云服务运营中心通过风险探知系统对我国境内部署 Microsoft DNS 的服务器进行统计，结果显示我国境内的 Microsoft DNS 的服务器约有 32048

台。按区域统计来看，排名前五的省份或地区为台湾省、广东省、香港特别行政区、北京市、上海市。

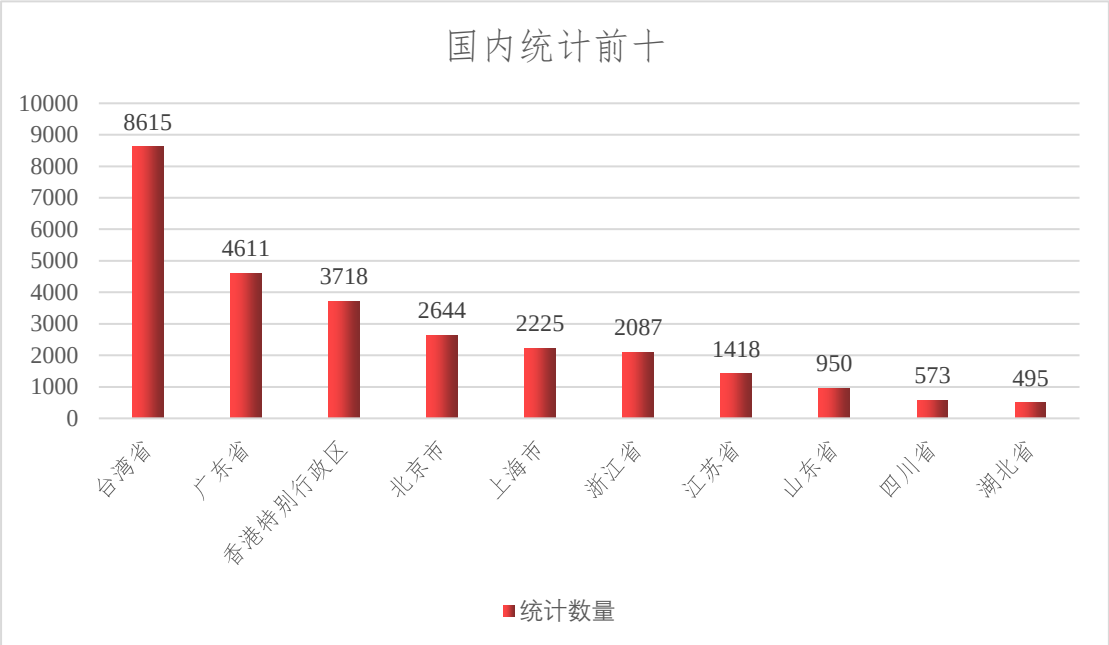

图 26 国内统计前十

按运营商统计来看，排名前五的运营商分别为电信、中华电信、联通、阿里云、腾讯网络。

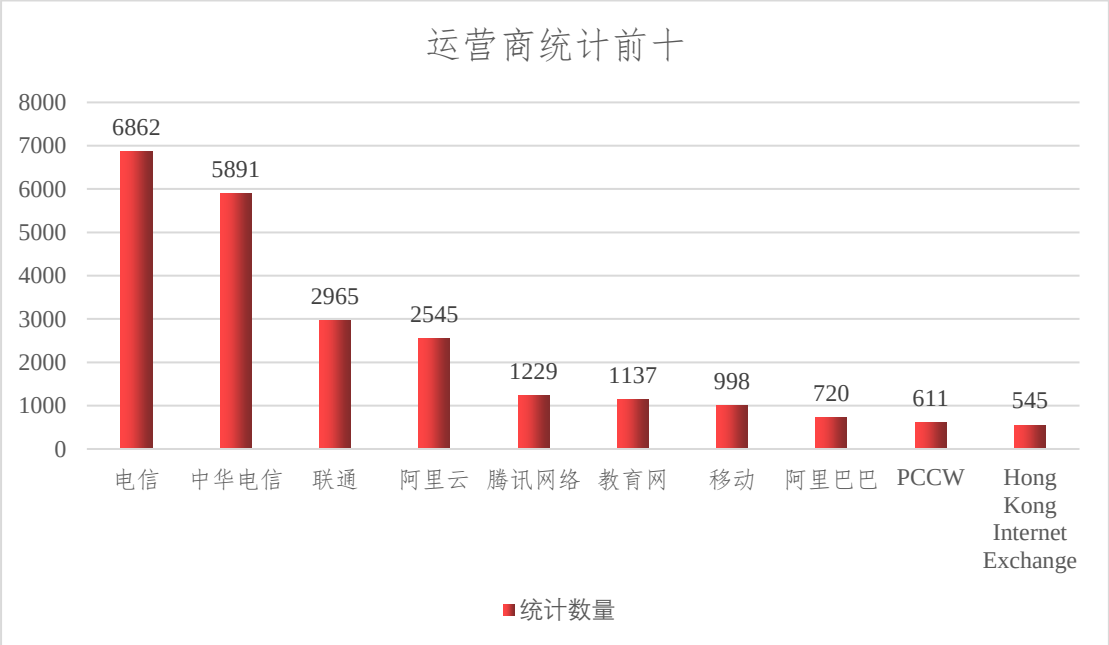

图 27 运营商统计前十

8. SQL Server 远程代码执行漏洞

1）漏洞描述

2020 年 02 月 16 日，在微软 2 月份的安全更新中发现 SQL Server 远程命令执行漏洞（CVE-2020-0618）。SQL Server 是 Microsoft 公司推出的关系型数据库管理系统，是一个全面的数据库平台。

要利用该漏洞需要经过身份验证后，向受影响的 SQL Server 的报告服务(Reporting Services) 发送精心编制的页面请求。成功利用此漏洞的攻击者可以在 SQL Server 服务的上下文中执行代码。

本次漏洞影响了 Microsoft SQL Server 2012、2014 以及 2016 版本，SQL Server 在国内外拥有众多用户，该漏洞在全球范围内具有较大的威胁。

2）数据分析

天融信安全云服务运营中心通过风险探知系统对我国境内部署 SQL Server 数据库的服务器进行统计，结果显示我国境内的 SQL Server 服务器有 8.2 万余台。按区域统计来看，排名前三的省份是浙江省 3 万余台，北京市 1 万 6 千余台，广东省 1 万 3 千余台。由此可见 SQL Server 在国内用户众多，该漏洞具有较大威胁。

9. F5 BIG-IP TMUI 远程代码执行漏洞

1）漏洞描述

F5 BIG-IP 是美国 F5 公司的一款集成网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。

攻击者利用该漏洞，通过向 TMUI 发送恶意攻击请求，从而执行任意系统命令、创建或删除文件、禁用服务，以及执行任意 Java 代码，最终完全获取系统权限。该漏洞影响了 F5 BIG-IP 众多版本，在受影响的版本中，F5 BIG-IP

Appliance 模式下的 BIG-IP 系统也受到漏洞影响。但此漏洞不影响数据面板，只影响控制面板。

2）数据分析

天融信安全云服务运营中心对中国境内的 F5 BIG-IP 设备进行了抽样数据统计及分析，数量约为 1.4 万余台。其中，排名前五的省份或地区分别为：北京市、广东省、上海市、香港特别行政区、台湾省。

下图为国内 F5 BIG-IP 设备统计数量排名前十的情况：

图 28 国内统计排名前十

下图为国内 F5 BIG-IP 设备的运营商统计数量排名前十的情况：

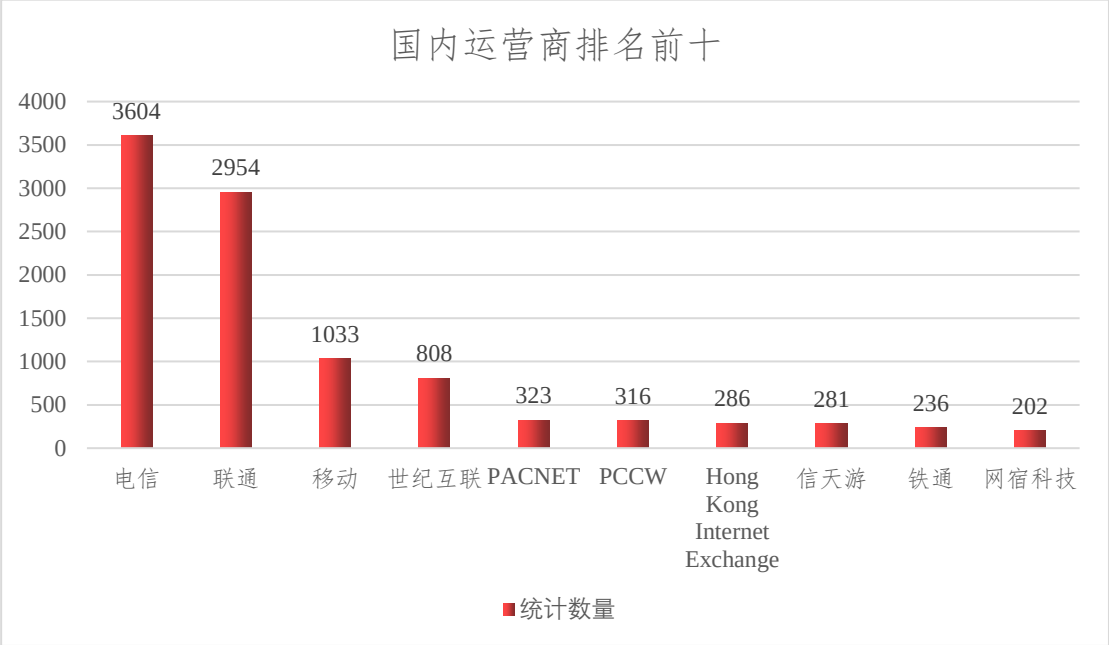

图 29 运营商统计前十

10. Apache Dubbo 远程代码执行漏洞

1）漏洞描述

Apache Dubbo 是一个高性能优秀的服务框架，使得应用可通过高性能的 RPC 实现服务的输出和输入功能，可以和 Spring 框架无缝集成。Dubbo Provider 存在 反序列化漏洞，攻击者可以通过 RPC 请求发送无法识别的服务名称或方法名称以及一些恶意有效载荷，当恶意参数被反序列化时，可以造成远程代码执行。

Apache Dubbo 作为一个优秀的服务框架被广泛使用，该漏洞影响了 Dubbo 2.7.0 - 2.7.6、2.6.0 - 2.6.7、2.5.x 版本，在全球范围内具有较大的威胁。

天融信阿尔法实验室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/apache-dubbo-cve-2020-1948-%e5%8f%8d%e5%ba%8f%e5%88%97%e5%8c%96%e8%bf%9c%e7%a8%8b%e4%bb%a3%e7%a0%81%e6%89%a7%e8%a1%8c%e6%bc%8f%e6%b4%9e%e5%8f%8a%e5%85%b6%e8%a1%a5%e4%b8%81%e7%bb%95%e8%bf%87%e6%b7%b1/

2）数据分析

天融信安全云服务运营中心通过风险探知系统对我国境内部署 Apache Dubbo 的服务器进行统计，结果显示我国境内的 Microsoft DNS 的服务器约有 400 台。按区域统计来看，排名前五的省份或地区为广东省、浙江省、北京市、上海市、陕西省。

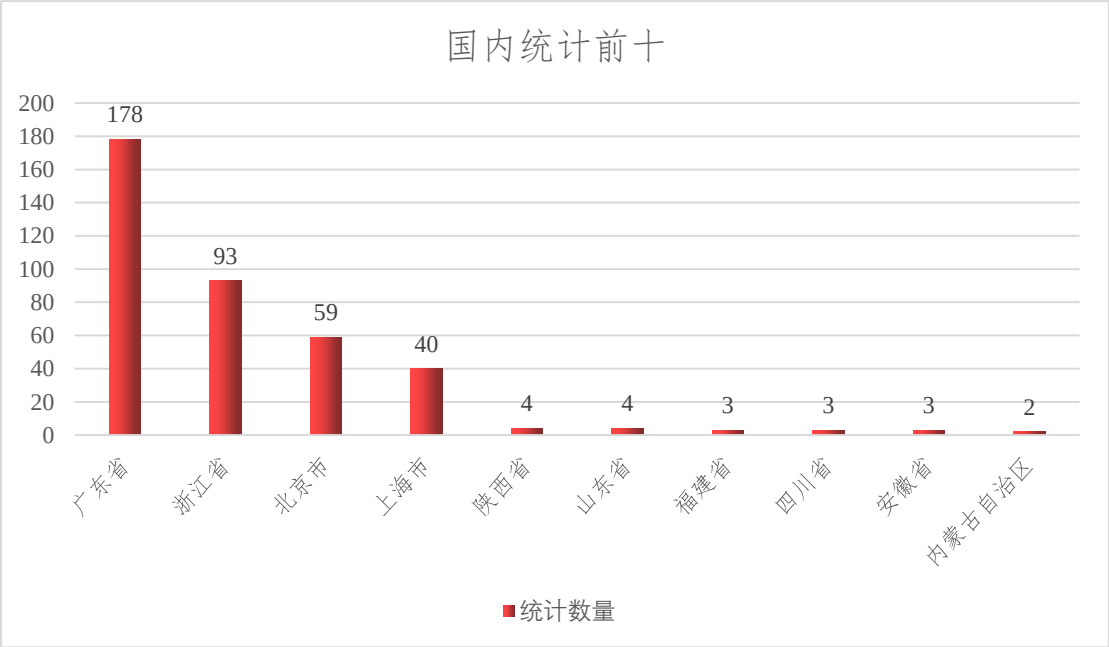

图 30 国内统计前十

按运营商统计来看，排名前五的运营商分别为阿里云、阿里巴巴、电信、腾讯网络、移动。

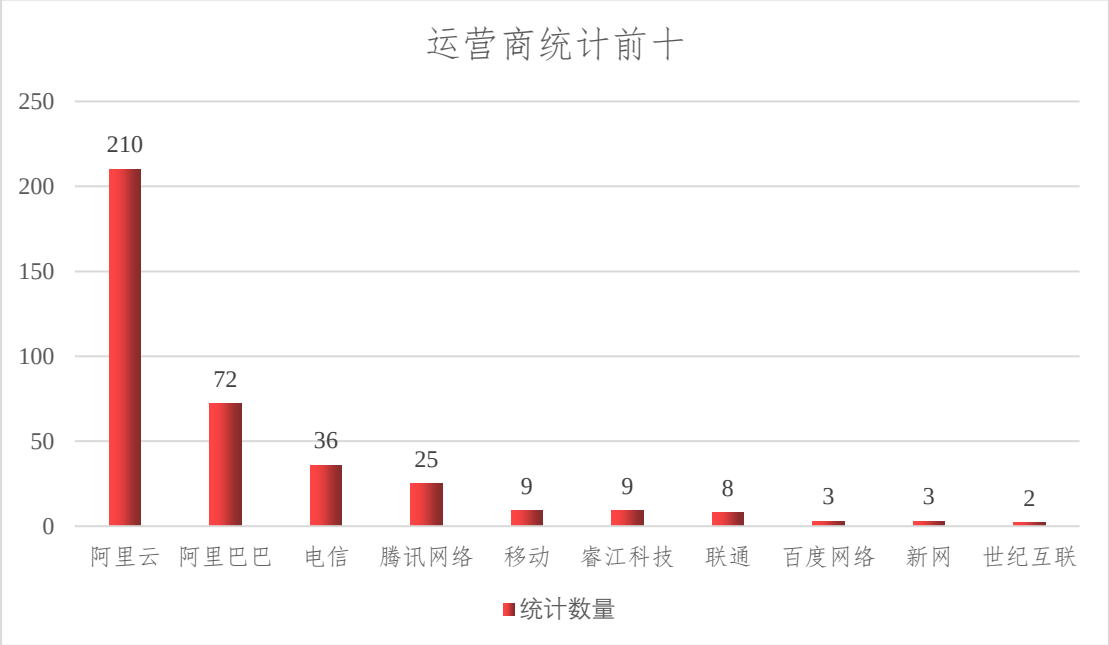

图 31 运营商统计前十

按端口统计数量来看，排名前五的端口分别为 7070、6060、1099、9002、20000。

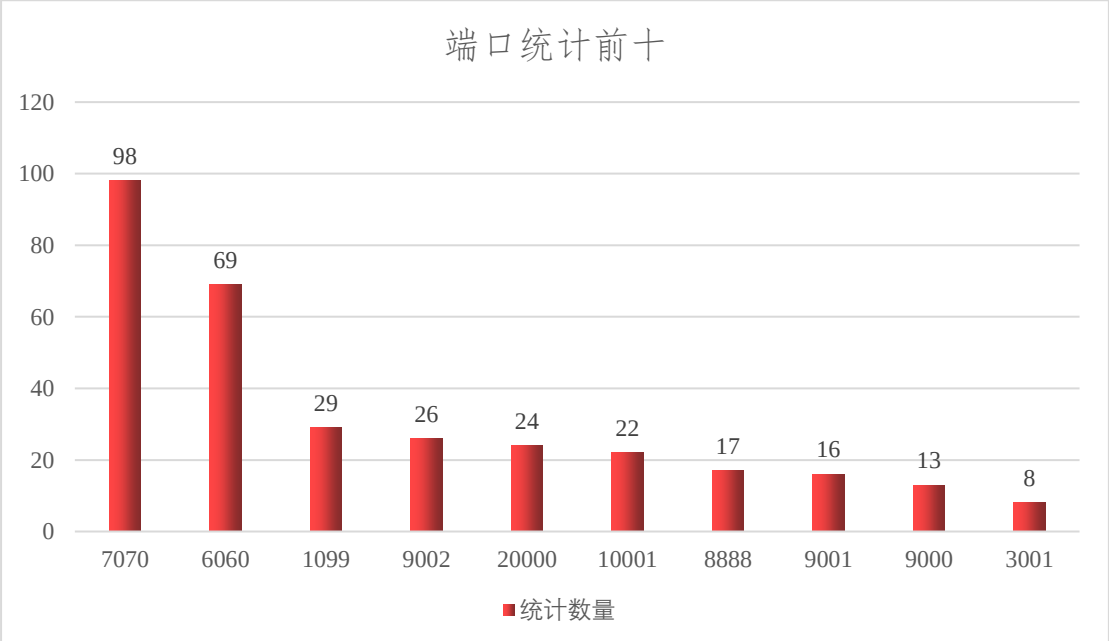

图 32 端口统计前十

五、总结

同往年相比，2020 年漏洞数量快速增长，漏洞的激增表明企业在大规模开展业务的同时却难以管理业务自身所带来的网络风险。近年来，由漏洞所带来的各种勒索病毒事件、 APT 攻击事件、数据泄露事件比比皆是，对企业以及个人安全造成了严重的威胁。

纵观 2020 年的高危漏洞，具有以下几个趋势，第一是漏洞跨度广泛，主流操作系统、流行网络协议、底层 TCP/IP 协议库、知名 WEB 容器和开发框架以及网络安全设备均被发现存在安全漏洞。第二是漏洞类型广泛，远程代码执行、反序列化、命令执行及权限提升等具有严重影响的安全漏洞具有较高占比。第三则是部分漏洞被恶意利用可能性更大，据统计有相当一部分高危漏洞的 POC 在互联网上公开流传，攻击者基于这一类信息可以进一步开发漏洞利用工具，给网络安全造成实际威胁。

基于 2020 年安全漏洞的发展趋势，我们建议：安全运维人员在部署网络服务时应做好权限访问控制，减少对外部网络暴露组件接口的情况。关注网络安全资讯，及时排查受漏洞影响的网络服务；终端用户应及时进行系统及应用软件的安全更新，避免遭受公开漏洞的安全威胁；安全厂商除了关注安全产品的核心功能，还应特别重视产品自身的安全问题，避免因产品漏洞导致安全堡垒被攻破。

可以预见，在即将到来的 2021 年中，漏洞数量尤其是高危漏洞的数量将继续呈现持续增长的状态。随着安全人员对其关注度的日益增加，相关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。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。于此同时，应将代码审计等环节添加到软件的开发过程中。 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。

关于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。