H3C
数字化解决方案领导者

新华三主动安全

2021年
网络安全漏洞态势报告

新华三信息安全技术有限公司
新华三攻防实验室
2022年3月

目　录

2021 年网络安全漏洞态势报告

新华三攻防实验室持续关注国内外网络安全漏洞和态势，协同高级威胁分析、漏洞分析、威胁情报分析等领域专家一同发布《2021 年网络安全漏洞态势报告》。报告开篇概述了 2021 年漏洞和攻击的总体趋势，正文从 Web 应用、操作系统、网络设备、数据库、工控系统、云计算平台多个角度分析了漏洞分布和攻击态势。本报告试图以观察者的视角剖析 2021 年网络安全领域新增漏洞情况以及演变趋势，希望为各行业及相关企事业单位的网络安全建设提供参考和帮助。

1 概述

1.1 漏洞增长趋势

2021 年新华三收录的漏洞总数为 20203 条，其中超危漏洞 2591 条，高危漏洞 8451 条，如图 1 所示，超危与高危漏洞占比 50%以上，如图 2 所示，高危以上漏洞比 2020 年增长 14.3%。2016 年至 2021 年漏洞总体呈逐年增长趋势，其中高危以上漏洞逐年增长比例超过 10%。

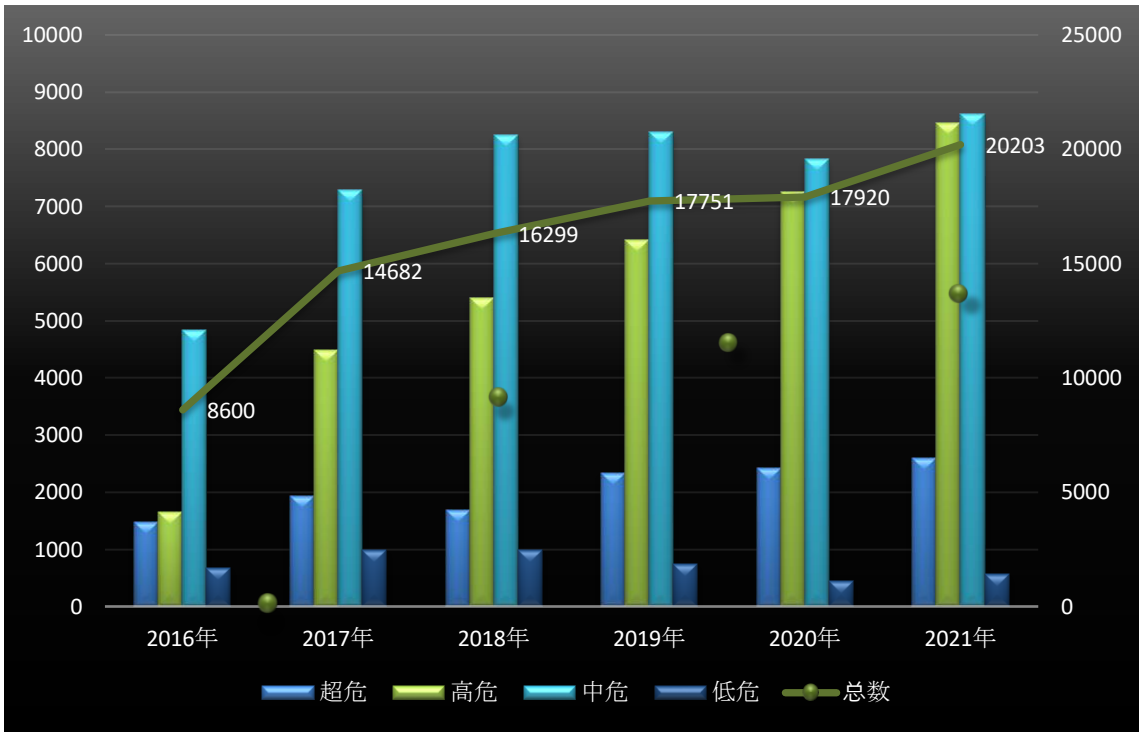

图 1 2016-2021 年新增漏洞总趋势

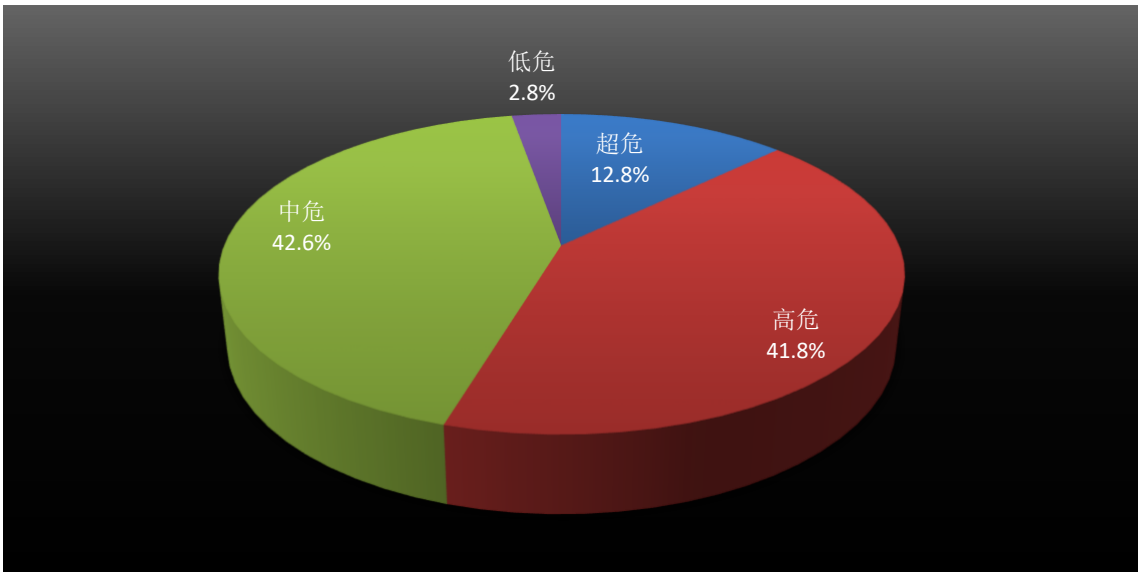

图 2 2021 年不同危险级别漏洞占比

1.2 攻击总体态势

新华三攻防实验室在 2021 年根据跟踪的热门及严重漏洞，新增 2021 年漏洞的防御规则 710 多条，其中超危漏洞占比 17.1%，高危漏洞占比 53.2%，两者占比高达 70.3%，含有 CVE 的漏洞为 428 条，占比 60%，非 CVE 漏洞占比增加。将新增漏洞规则按照攻击对象进行统计，Web 应用类漏洞占比最高，达到 48.1%，Web 应用类包括 OA 系统、CMS 系统，2021 年其漏洞仍然呈高发态势；网络设备类漏洞占比高达 12.2%，近两年利用网络设备、安全设备漏洞进行内网攻击的事件屡见不鲜，网络设备自身安全不容忽视。

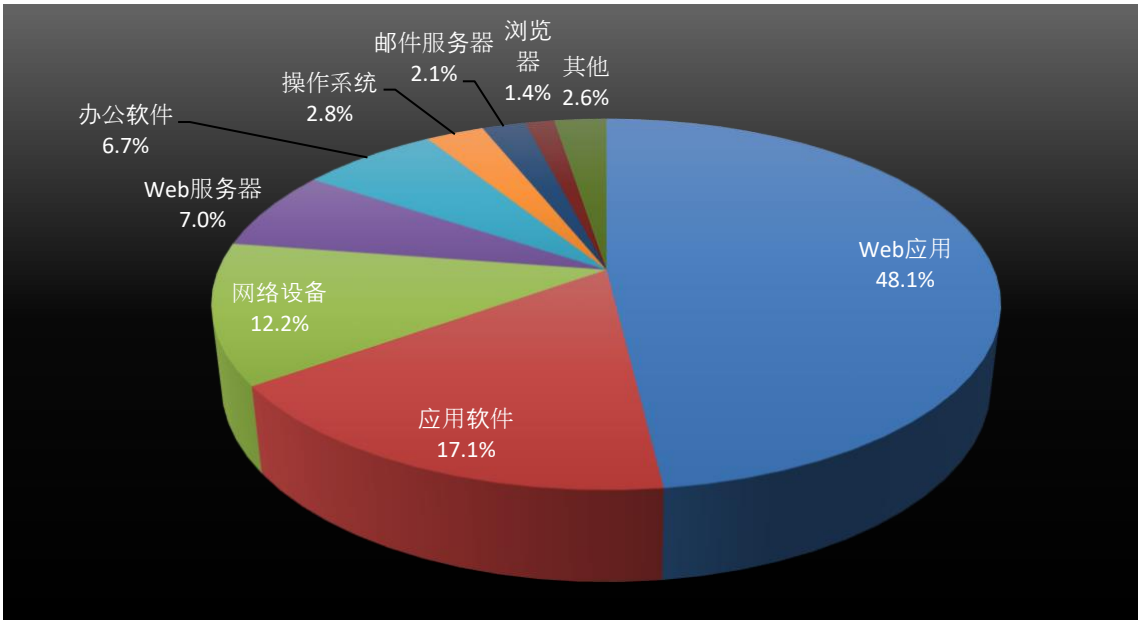

图 3 2021 年新增规则保护对象占比

将新增漏洞规则按照攻击分类进行统计，远程代码执行类占比最高，达到 32.7%，命令注入、SQL 注入占比也较高，分别为 10.8%和 8.0%。远程代码执行、命令注入为高风险漏洞，如果攻击成功可以直接执行攻击者注入的代码或命令。

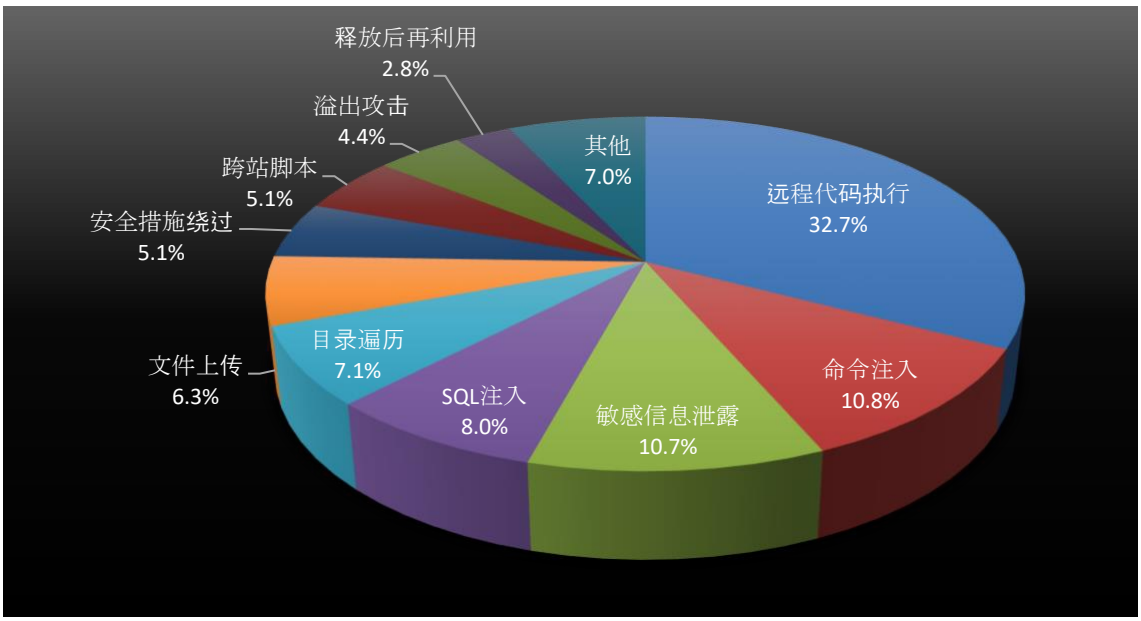

图 4 2021 年新增规则攻击种类占比

根据对 2021 年攻击进行的观察，我们得出一些结论：

(1) 供应链安全威胁增加，供应链攻击成为网络空间常态

当前，供应链攻击是世界各国网络空间领域普遍面临的一个最显著威胁之一。供应链攻击是一种危害和破坏性极强的网络攻击，是针对组织供应链（上游、中游、下游）中的薄弱环节实施的网络安全攻击，涉及范围广，且难以检测。

供应链攻击存在难发现、难溯源、难清除等特点，这暴露出网络安全领域“易攻难守”的非对称性特征。2020 年 12 月，震惊全球的美国太阳风事件，就是网络攻击者从美国软件供应链厂商下手，从而实现对美国众多高涉密政府机构的网络渗透。2021 年 3 月，SITA 通报了一起数据泄露事件，马来西亚航空公司常客计划的 58 万多条记录遭遇泄露，SITA 为全球 90%的航空公司提供服务，此次事件之后，全球多家航空公司遭遇数据泄露，事件蔓延至整个供应链。2021 年 4 月，澳大利亚公司 ClickStudio 遭受了软件供应链攻击，攻击者入侵了该公司的密码管理器 Passwordstate，并植入了恶意代码，ClickStudio 在全球拥有约 29 , 000 个企业和政府客户，涉及航空航天、银行、国防、医疗、公用事业和其他行业。2021 年 10 月，开源的代码质量管理平台 SonarQube 被黑客攻破，使得很多公司和机构开始紧急排查其设备或系统是否集成了 SonarQube，其中不乏一些国家机关单位。2021 年 12 月席卷全球的 Log4j 漏洞，其影响范围之广，危害性之大都是史诗级程度，甚至有人将该漏洞称为“核弹级”漏洞，其威胁性可见一斑，Log4j2 漏洞背后可以说是全球软件供应链风险面临失控的状况。供应链的各个环节及其薄弱点都可能成为攻击者的切入点和重点目标，这些攻击既可涉及系统和业务漏洞、非后门植入、软件预装等，也可能涉及更高级的供应链预制问题。当前针对这一安全问题，已经有不少国家都出台了新的政策法规来指导本国的供应链安全管理，以提高供应链安全韧性。

(2) 有针对性的勒索攻击呈上升趋势，勒索赎金水涨船高

勒索软件攻击被认为是 2021 年一年中最具威胁性的侵害事故，全球网络遭受了勒索软件攻击以及有组织的黑客行动的轮番轰炸，攻击目标遍及医疗、金融、制造业、电信及交通等重点行业，数据泄露的规模、影响设备的数量、破坏效果呈扩大趋势。勒索攻击对象涉及面越来越广，目前主要针对掌握大量数据的大型企业，且定向精准攻击趋势愈发明显，有针对性的勒索软件攻击呈上升趋势，例如通过企业财务报表或新闻搜索能够获得足够支付能力的企业，或在感染勒索软件的情况下可能因服务中断而导致大规模业务损失的企业等，都可能成为勒索软件攻击的主要目标。

2021 年 3 月底，美国最大的保险公司之一 CNA Financial 被勒索软件攻击，在试图恢复文件无果之后，他们开始与攻击者谈判，黑客要求的赎金高达 6000 万美元。最后，CNA Financial 在事件发生两周后支付了 4000 万美元赎金，以重新获得对其网络的控制权。2021 年 5 月，美国最大燃油管道 Colonial Pipeline 勒索软件攻击事件导致美国最大的成品油管道运营商关闭整个能源供应网络，政府宣布进入国家紧急状态，Colonial Pipeline 公司向 DarkSide 勒索软件组织支付了 440 万美元赎金；在同一月份，全球最大肉类加工企业 JBS FOODS 勒索软件攻击事件导致其加工厂全球多地停产，公司向网络犯罪分子支付了 1100 万美元赎金。2021 年 7 月，美国软件开发商 Kaseya 遭勒索攻击，声称有超过 100 万台设备遭到感染，网络攻击团伙索要高达 7000 万美元的赎金。

(3) 针对各种物联网设备的网络威胁日益增加

随着物联网设备的普及，家用摄像头、智能电视等物联网设备被黑客入侵，偷拍的私生活视频被黑客泄露，甚至被拿到暗网上进行出售等，网络威胁已渗透到日常生活中的方方面面，成为一个严重的社会问题。不同于虚拟的互联网，物联网与现实生活息息相关，如果说以前的网络威胁只针对企业等有限范围内发生了攻击并造成了损失，那么今后的网络威胁正在逐渐演变成威胁人们自身安全的形态。

除了 AI 音箱、智能电视和 IP 相机等已知的物联网设备之外，针对无人机、智能汽车等新型物联网设备的安全威胁也正在成为现实。不同于 PC 端、手机端，物联网设备的安全防护水平通常不高，用户没有相关的杀毒软件可以使用。如果物联网设备的安全性如此脆弱，很有可能被恶意利用为隐私信息泄露或 DDoS 攻击等网络攻击的手段，因此物联网设备提供商理应提供更高等级的安全防护。

事实上，猖獗的物联网攻击行为也引起了有关部门重视。2021 年 6 月 11 日，中央网信办、工业和信息化部、公安部、市场监管总局发布《关于开展摄像头偷窥等黑产集中治理的公告》，自 2021 年 5 月至 8 月，在全国范围组织开展摄像头偷窥黑产集中治理。其中，公告第二条就明确要求，摄像头生产企业要按照数据安全、信息安全有关规定和标准提升产品安全能力，提供公共服务的视频监控云平台及有关企业要严格履行网络安全主体责任，强化云平台网络安全防护，落实对远程视频监控 APP 的数据安全防护责任。

(4) 云计算环境安全威胁增加

随着各种信息通信环境（如服务、平台和基础设施等）正在向基于云计算的数字化转型，在这种情况下恶意利用云计算环境的安全威胁也将增加。云计算蕴含着资源共享、虚拟化等特性所带来的安全威胁，并且由于云计算中积累了大量的 IT 资源及用户信息，很容易成为黑客攻击和 DDoS 攻击的目标，一旦发生安全事故可能会造成大规模的损失。研究人员发现，目前有将近数万个云端账号正在暗网市场上廉价出售，而这些云资源也为网络犯罪分子提供了很多攻击切入点。报告显示，暗网市场上目前有近 3 万个已被入侵的云账号，销售价格从几美元到几万美元不等，具体取决于云资

源的地理位置、账户上的信用额度和账户访问级别，而且暗网商家还提供了诱人的退款政策来吸引买家进行购买。

(5) 恶意利用社会焦点问题的黑客电子邮件增加

由于疫情影响，突然转向远程办公模式导致许多企业将他们的电子邮件迁移到云平台，大大地增加了攻击面。企业拥有比以往任何时候都多得多的接触点，如果没有额外的安全保护措施，云电子邮件很容易受到凭据式网络钓鱼、勒索软件和其他恶意攻击。黑客电子邮件利用新冠肺炎疫情、政治局势等社会焦点问题，以窃取个人信息、甚至进行电信金融诈骗的攻击活动持续发生。特别是，通过分析窃取的个人信息，并以巧妙手段欺骗收信人以免引起怀疑的智能化鱼叉式网络钓鱼案件持续增加。

据统计，2021 年，将近一半的发往收件箱的电子邮件被归类为垃圾邮件，企业用户最常受到窃取凭据的网络钓鱼攻击，电子邮件通常伪装成商业信函或需要收件人注意的有关工作文件的通知。同时还有会议的虚假通知，或有关以批准工资支付的重要文件的消息。但是，COVID-19 在 2021 年中仍然是网络钓鱼者的一个持久主题。

(6) 零日攻击威胁日益增长

虽然大多数攻击继续利用已知漏洞，但网络犯罪分子也在加倍努力瞄准新漏洞。例如 2021 年 1 月，黑客组织 Hafnium 开始利用微软 Exchange Server 中的七个新漏洞，比补丁发布时间早了两个多月。虽然微软之前已经发现了其中三个漏洞，但有四个是未知的零日漏洞。Hafnium 的自动化攻击主要针对未打补丁的 Exchange 服务器，然后使用设计好的 Webshell 远程控制恶意软件、窃取数据、并未经授权访问关键系统。全球数以万计的组织受到影响，包括总部位于美国的组织，如律师事务所、国防承包商、进行传染病研究实验室和非政府组织。

2 Web 应用漏洞

全球进入数字驱动的新经济发展期，人工智能、自动驾驶、区块链、物联网、工业互联网等技术飞速发展，全球贸易和科技面临新的竞争格局。而网络空间承载着技术创新突破、数据资源争夺、国家利益角逐等多重多维职能，其安全问题的战略价值日益突出。Web 应用由于其自身的公开属性，涉及的攻击面广且远程利用方式相对简单，一直都是网络攻击的重灾区。2021 年新华三共收录 Web 应用漏洞 9103 条，较 2020 年（6145 条）增长 48.1%，漏洞数量大幅增长。对比 2020 年和 2021 年每月 Web 应用漏洞变化趋势如图 5 所示：

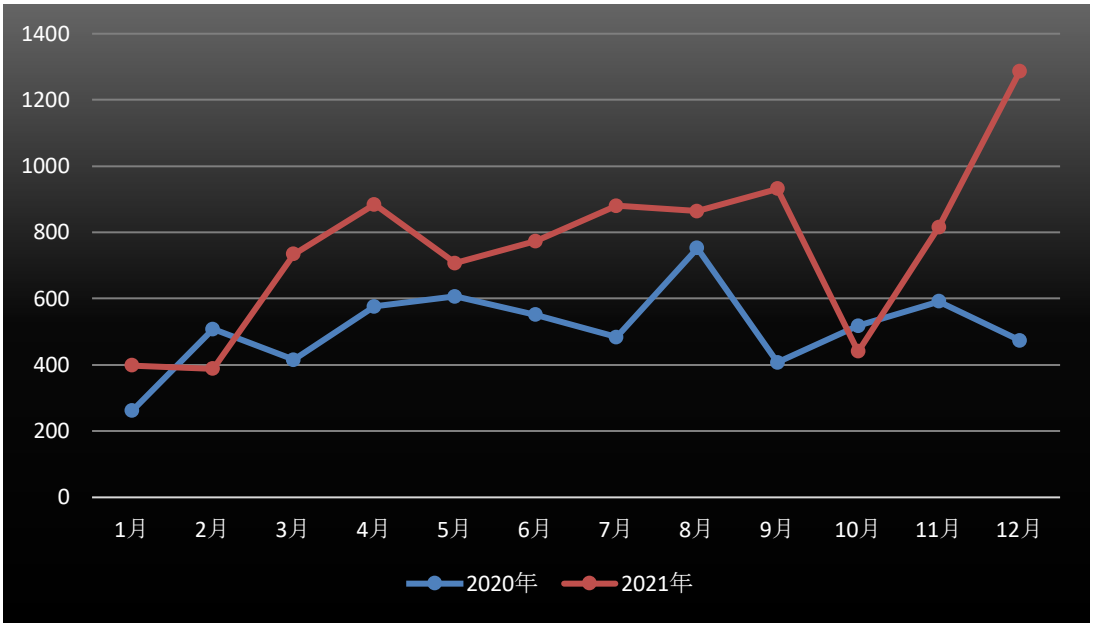

图 5 2020 与 2021 年 Web 应用新增漏洞趋势

2.1 漏洞分类

Web 应用由于其自身的公开属性，涉及的攻击面广且远程利用方式相对简单，一直都是遭受网络攻击的重灾区，可以看出 Web 应用漏洞主要集中在跨站脚本、注入、失效的身份验证、敏感数据泄露四种类型，占据全部漏洞类型的 73.6%。

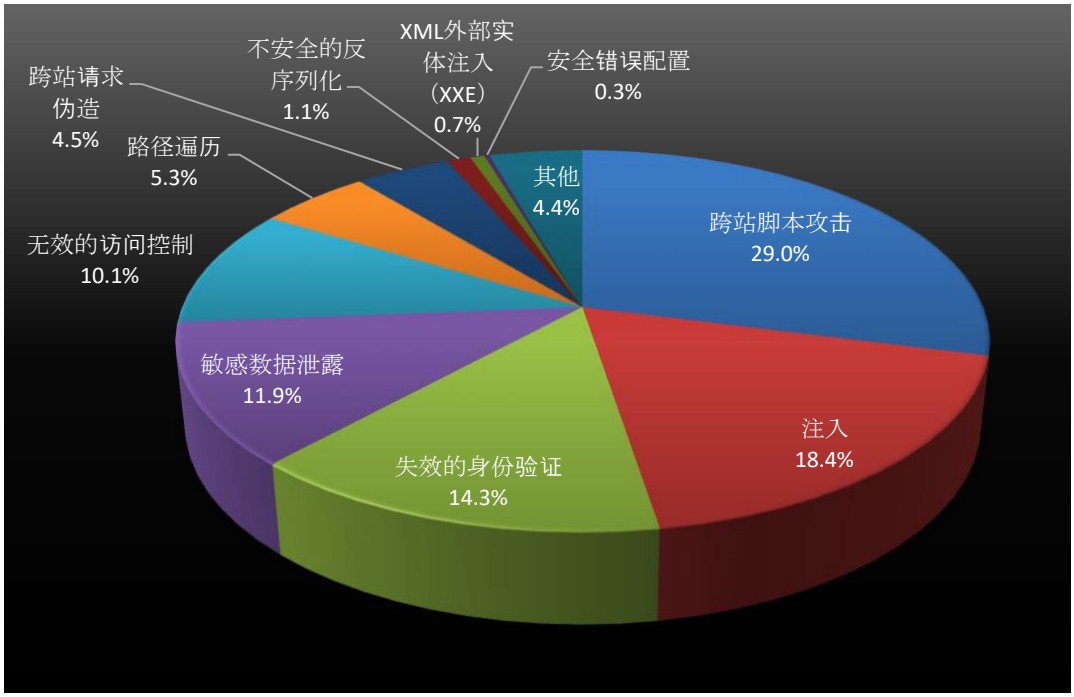

图 6 2021 年 Web 应用漏洞类型占比

2.2、重点漏洞回顾

漏洞名称	发布时间
FasterXML Jackson-databind反序列化漏洞	2021/01/08
Oracle Weblogic Server JNDI注入漏洞（CVE-2021-2109）	2021/01/20
Apache Druid远程代码执行漏洞（CVE-2021-25646）	2021/01/29
Node.JS命令注入漏洞（CVE-2021-21315）	2021/02/16
Apache OFBiz RMI不安全反序列化（CVE-2021-26295）	2021/03/22
XStream远程任意代码执行漏洞（CVE-2021-21347）	2021/03/22
Ntopng权限绕过漏洞（CVE-2021-28073）	2021/03/25
Apache Solr 服务端请求伪造漏洞（CVE-2021-27905）	2021/04/13
Apache HTTP Server路径遍历漏洞（CVE-2021-41773）	2021/04/13
Apache Tapestry未授权访问漏洞（CVE-2021-27850）	2021/04/15
Oracle Weblogic Server反序列化漏洞(CVE-2021-2135)	2021/04/19
GitLab远程代码执行漏洞（CVE-2021-22205）	2021/04/22
Apache OFBiz远程代码执行漏洞（CVE-2021-29200）	2021/04/27
Apache OFBiz反序列化远程代码执行漏洞（CVE-2021-30128）	2021/04/27
Apache Dubbo RPC反序列化远程代码执行（CVE-2021-25641）	2021/06/01
YAPI远程代码执行漏洞	2021/07/08
Oracle Weblogic Server反序列化漏洞(CVE-2021-2394)	2021/07/19
Atlassian Confluence远程代码执行漏洞（CVE-2021-26084）	2021/08/27
Apache mod proxy SSRF漏洞（CVE-2021-40438）	2021/09/16
PHPFusion远程代码执行漏洞（CVE-2021-40189）	2021/10/11
Apache ShenYu 授权漏洞（CVE-2021-37580）	2021/11/16
Apache Log4j2远程代码执行漏洞（CVE-2021-44228）	2021/12/10
Apache Log4j2拒绝服务漏洞（CVE-2021-45105）	2021/12/18

Apache Log4j2 JMSAppender远程代码执行漏洞 (CVE-2021-4104)	2021/12/13
Apache Log4j2远程代码执行漏洞 (CVE-2021-44832)	2021/12/28

经典漏洞盘点：

- FasterXML Jackson-databind 反序列化漏洞

2021 年 1 月 8 日，jackson-databind 官方发布 jackson-databind 公告，通报了 11 个反序列化漏洞，漏洞编号为 CVE-2020-36179 至 CVE-2020-36189。Jackson 是美国 FasterXML 公司的一款适用于 Java 的数据处理工具，jackson-databind 是其中的一个具有数据绑定功能的组件。当开发人员在应用程序中通过 ObjectMapper 对象调用 enableDefaultTyping 方法时，程序就会受到此漏洞的影响。攻击者可通过发送特制的 JSON 消息利用该漏洞执行任意代码，直接获取服务器控制权限。

- Oracle Weblogic Server 反序列化漏洞

2021 年 1 月 20 日，Oracle 官方发布了 2021 年 1 月份关键补丁更新公告，包含 329 个安全补丁，其中涉及 7 个 CVSS 评分为 9.8 的 Weblogic Server 的高危漏洞(CVE-2019-17195、CVE-2021-1994、CVE-2021-2047、CVE-2021-2064、CVE-2021-2108、CVE-2021-2075、CVE-2020-14756)，利用复杂度低，未经身份验证的攻击者可构造恶意请求，造成 JNDI(Java Naming and Directory Interface)注入，执行任意代码，从而控制服务器。

其中 CVE-2020-14756 反序列化漏洞，未经身份验证的远程攻击者可通过 coherence 组件中的类绕过黑名单检测机制，从而重新利用黑名单中的类构造序列化数据导致恶意代码执行。而在这次修复补丁中仅针对实现了 JEP290 的 JDK 提升了安全性。2021 年 4 月 19 日披露 CVE-2021-2135 反序列化漏洞，该漏洞为 CVE-2020-14756 的补丁绕过，攻击者无需身份认证构造特定 T3、IIOP 协议序列化数据传输到服务端即可执行任意代码，在这次的补丁中除了增加黑名单外，还引入了对 T3 协议的白名单防护。2021 年 7 月 19 日披露 CVE-2021-2394 反序列化漏洞，由于上一次修复中 IIOP 协议没有进行白名单过滤，故目前网上披露的利用细节都是利用 IIOP 协议构造新的利用链来触发此漏洞。同时在这次修复中除了增加黑名单列表外，也将处理 IIOP 协议的输入流 IIOP InputStream 进入反序列化逻辑前进行了转化。

- Node.JS 命令注入漏洞 (CVE-2021-21315)

Node.js 是一个基于 Chrome V8 引擎的 JavaScript 运行环境，使用了一个事件驱动、非阻塞式 I/O 模型，让 JavaScript 运行在服务端的开发平台，它让 JavaScript 成为与 PHP、Python、Perl、Ruby 等服务端语言平起平坐的脚本语言。在 Node.js 解析传入的 RST_STREAM 帧（用于终止连接）时，由于对接收到的 RST_STREAM 帧的处理中没有错误代码和取消错误代码(nghttp2_cancel)，接收器将试图强制清除收到的任何现有数据，完成后会自动回调运行另外的“关闭”函数，尝试第二次释放内存，从而导致 nghttp2 关闭已经破坏的流，触发双重释放错误。攻击者可利用该漏洞实现应用程序崩溃或远程代码执行。

- SaltStack 未授权远程代码执行漏洞 (CVE-2021-25281)

SaltStack 是基于 python 的开发的一套 C/S 架构的运维管理工具，运用此工具容易管理上万台服务器，具有部署简单，通信速度快等优点，广泛运用于云计算、自动化运维领域。2021 年 02 月 26 日，SaltStack 官方发布安全更新，修复了包含 CVE-2021-25281 在内的多个高危漏洞。由于 CVE-2020-17490 的补丁修补不完整，导致 wheel_async 仍然存在未授权访问，可以调用 wheel 模块中

的方法，加载配置模块存在模板注入，可以实现未授权远程代码执行。通过相关漏洞组合利用，未经身份验证的攻击者可远程触发漏洞，成功利用这些漏洞可在目标机器上执行任意代码。

- Apache Log4j2 远程代码执行漏洞 (CVE-2021-44228)

Log4j 是 Apache 的一个开源项目，它允许开发者以任意间隔输出日志信息，控制每一条日志的输出格式，通过定义每一条日志信息的级别，还能够更加细致地控制日志的生成过程。2021 年 12 月 9 日，网上爆发了 Apache Log4j 的任意代码执行漏洞(CVE-2021-44228)，成功利用此漏洞可以在受害主机上执行任意代码。2021 年 12 月 15 日，Apache Log4j 官方发布 Apache Log4j 远程代码执行漏洞(CVE-2021-45046)安全通告，完善了非默认配置下对 CVE-2021-44228 修复措施不完整问题。2021 年 12 月 18 日，Apache Log4j 官方发布 Apache Log4j 拒绝服务攻击漏洞(CVE-2021-45105)安全通告，修复了在非默认配置下自引用查找导致的无限循环问题，该漏洞可能导致拒绝服务攻击。2021 年 12 月 29 日，Apache Log4j 官方发布 Apache Log4j 远程代码执行漏洞(CVE-2021-44832)安全通告，攻击者可利用该漏洞修改日志配置实现远程代码执行。

2.2 攻击态势分析

(1) 组件漏洞波及范围广，从补丁通告到被绕过、再次修补愈发频繁

软件系统开发过程中，在已有知名组件可满足所需功能时，考虑到知名组件经历多次分析挖掘、问题修复、迭代优化，一定程度上安全性较高，结合时间、成本、效率、稳定性及可维护性等因素，企业大多数情况下会直接采用或进行二次开发。但同时，鉴于其使用广泛，可获取的信息多，方便安全研究人员进行多角度分析，一旦组件出现漏洞，组件信息较为明确，不同行业不同系统都可被快速扫描利用。

由于影响面大，安全人员参与程度高，不同网站环境利用方式迥然不同，在无法完整评估所有利用情况的前提下，修复补丁可被多次绕过利用，短时间内无法一次性解决，可被批量利用。

例如 Oracle 在 2021 年 1 月、4 月、7 月发布的关键补丁更新公告中，分别包含 CVE-2020-14756、CVE-2021-2394 与 CVE-2021-2135 的漏洞修复，每次补丁公告都是由于上一次补丁修复不完全，可以被绕过。而针对 Apache Log4j 的漏洞补丁发布更频繁，2021 年 12 月，Apache Log4j 官方发布了四次安全通告，以修补 Log4j 的安全问题，其原因也是由于每次补丁修复不完全。

(2) 为了对抗安全设备，黑客工具趋向加密

随着红蓝对抗愈发激烈，攻击手法越来越多样，攻击技术也在不断提升。第一代 webshell 管理工具“中国菜刀”的交互流量特征突出，容易区分，各类安全设备均可对其检测。为了避免被网络边界防护设备封堵，攻击者通过对流量进行加密等方式绕过安全设备的检查，从冰蝎、哥斯拉 webshell 管理工具的更新很明显可以观察到这种发展趋势，通过采用 AES 加密算法进行流量加密，传统基于流量特征匹配的网络安全设备已无法准确检测到此类恶意行为。

3 操作系统漏洞

操作系统作为传统的攻击目标，其漏洞占据着重要位置。2021 新华三收录的操作系统漏洞总数为 2439 条，较 2020 年总数（2343 条）稍有增长，对比 2020 年和 2021 年每月操作系统漏洞变化趋势如图 7 所示。

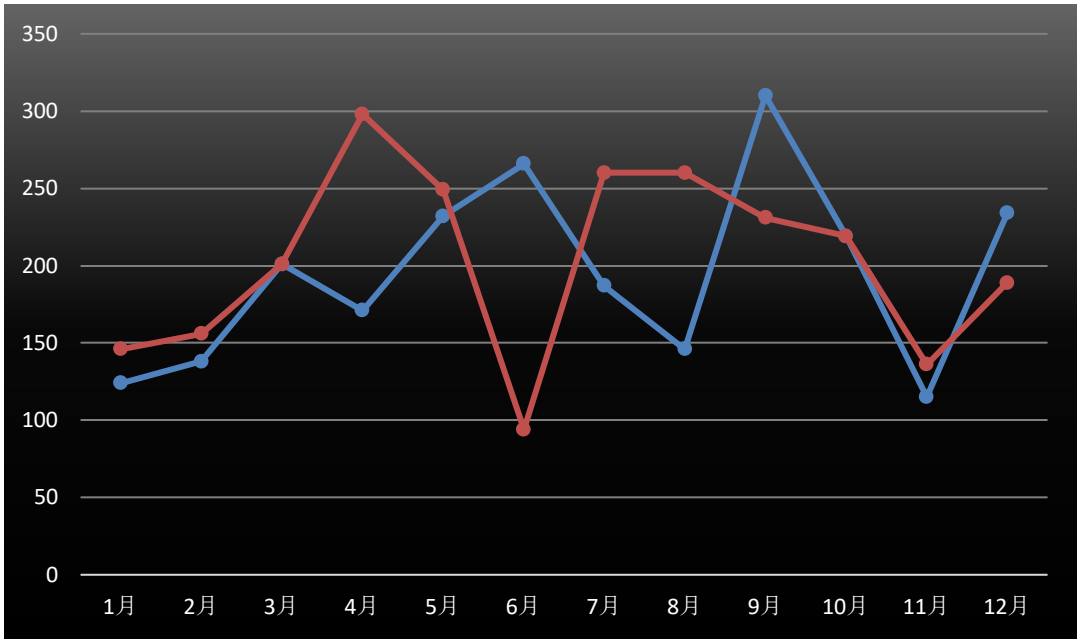

图 7 2020 与 2021 年操作系统新增漏洞趋势

3.1 漏洞分类

缓冲区溢出是一种非常普遍、非常危险的漏洞，在各种操作系统中广泛存在。利用缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是，它可被利用来执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作。2021 年缓冲区溢出漏洞占比 20.8%，排名第一，同时权限提升、信息泄露、拒绝服务等安全漏洞问题也是操作系统最为突出的问题，如图 8 所示。

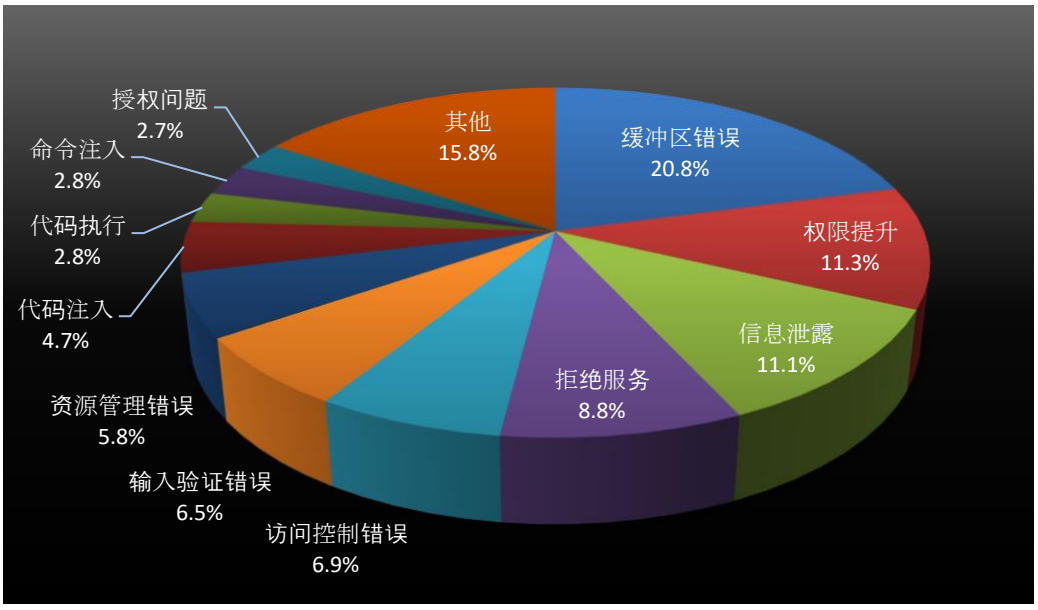

图 8 2021 年操作系统漏洞种类占比

3.2 重点漏洞回顾

漏洞名称	发布时间
Microsoft Windows Win32k 权限提升漏洞（CVE-2021-1709）	2021/1/12
Microsoft Windows Defender远程代码执行漏洞 (CVE-2021-1647)	2021/1/13
Microsoft Windows 10拒绝服务漏洞 (CVE-2021-28312)	2021/1/19
Sudo本地权限提升漏洞 (CVE-2021-3156)	2021/1/26
Windows TCP/IP拒绝服务漏洞 (CVE-2021-24086)	2021/2/9
Microsoft Windows Installer 本地权限提升漏洞（CVE-2021-1727）	2021/2/9
Microsoft Windows 本地权限提升漏洞（CVE-2021-1732）	2021/2/9
Microsoft Windows Win32k 本地权限提升漏洞（CVE-2021-1698）	2021/2/9
Microsoft Windows DirectX kernel driver 释放后重用漏洞（CVE-2021-24095）	2021/3/9
Microsoft Windows 权限提升漏洞（CVE-2021-26868）	2021/3/9
Microsoft Windows Win32k 权限提升漏洞（CVE-2021-26863）	2021/3/9
Microsoft Windows SMB Server SMBv2 SrvCreateBuildResponse信息泄露漏洞（CVE-2021-28325）	2021/4/13
Windows Graphics Component 权限提升漏洞（CVE-2021-31170）	2021/5/11
Microsoft Visual Studio 远程代码执行（CVE-2021-27068）	2021/5/11
Windows Graphics Component 权限提升漏洞（CVE-2021-31188）	2021/5/11
Windows Print Spooler远程代码执行漏洞 (CVE-2021-1675)	2021/6/30
Windows Print Spooler远程代码执行漏洞（CVE-2021-34527）	2021/7/1
Linux Kernel 文件系统层本地提权漏洞(CVE-2021-33909)	2021/7/20
Windows权限提升漏洞(CVE-2021-36934)	2021/7/22
Windows MS-EFSRPC协议NTLM中继攻击	2021/7/30

Windows Services for NFS ONCRPC XDR Driver远程代码执行漏洞（CVE-2021-26432）	2021/8/10
Windows Print Spooler远程代码执行漏洞(CVE-2021-36958)	2021/8/12
Microsoft MSHTML 远程代码执行漏洞 (CVE-2021-40444)	2021/9/7
Linux Kernel TIPC远程代码执行漏洞(CVE-2021-43267)	2021/11/2
Windows Active Directory域服务权限提升漏洞(CVE-2021-42278&CVE-2021-42287)	2021/12/14

经典漏洞盘点：

- Windows Print Spooler 远程代码执行漏洞 (PrintNightmare)

2021 年 6 月 9 日，微软发布 6 月安全更新补丁，修复了 50 个安全漏洞，其中包括一个 Windows Print Spooler 权限提升漏洞，漏洞 CVE 编号：CVE-2021-1675。Print Spooler 是 Windows 系统中用于管理打印相关事务的服务，虽然微软在公告中将该漏洞标记为 Important 级别的本地权限提升漏洞，但实际上在域环境中合适的条件下，无需任何用户交互，未经身份验证的远程攻击者就可以利用该漏洞以 SYSTEM 权限在域控制器上执行任意代码，从而获得整个域的控制权。

2021 年 7 月 1 日，微软发布了一个存在于 Windows 打印服务（Windows Print Spooler）的高危漏洞，CVE-2021-34527。漏洞根源在于 Windows Print Spooler 服务不正确地执行特权文件操作时，存在远程执行代码漏洞，攻击者可以通过一个低权限用户对目标计算机进行攻击，成功利用此漏洞的攻击者可以使用 SYSTEM 权限运行任意代码。然后攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。若攻击者获取到域用户权限，可连接到域控中的 Spooler 服务，并在域控制器中安装恶意驱动程序，从而完全控制整个域环境。

2021 年 7 月 15 日，微软发布安全公告称，发现一个影响 Windows Print Spooler 服务的安全漏洞，漏洞 CVE 编号为 CVE-2021-34481，CVSS 评分为 7.8 分。该漏洞是一个本地权限提升漏洞，攻击者利用该漏洞可以在系统中执行未授权的行为。攻击者成功利用该漏洞可以以 system 权限执行任意代码。然后攻击者可以安装程序、查看、修改和删除数据，或创建具有完全用户权限的新账户。

2021 年 8 月 10 日，微软发布了 2021 年 8 月份的月度例行安全公告，包含 CVE-2021-36936 Windows Print Spooler 远程代码执行漏洞，被列为“公开已知”，攻击者可利用该漏洞在受影响系统上执行代码。微软称利用该漏洞仅需低权限，因此它应该是非蠕虫漏洞，但用户仍应该优先测试并部署该严重漏洞。

2021 年 8 月 11 日，微软公布了一个新的 Windows Print Spooler 漏洞，编号为 CVE-2021-36958，将此漏洞归类为远程代码执行漏洞；攻击将允许攻击者安装程序、更改数据或创建新用户帐户。

PrintNightmare 漏洞的时间表：

CVE-2021-1675 - 2021 年 6 月 8 日修补

CVE-2021-34527 - 2021 年 7 月 7 日修补

CVE-2021-34481 - 2021 年 8 月 10 日修补

CVE-2021-34483 - 2021 年 8 月 10 日修补

CVE-2021-36936 - 2021 年 8 月 10 日修补

CVE-2021-36947 - 2021 年 8 月 10 日修补

CVE-2021-36958 - Microsoft 公告 2021 年 8 月 11 日。仅限缓解措施。

- Windows Active Directory 域服务权限提升漏洞

Microsoft Windows Active Directory 是美国微软（Microsoft）公司的一个负责架构中大型网络环境的集中式目录管理服务，目录服务（Active Directory 域服务 (AD DS) ）提供了一个分布式数据库，用于存储和管理来自目录的应用数据和网络资源数据信息。 2021 年 11 月 10 日 Microsoft 发布了十一月安全更新补丁，修复了 Microsoft 中多个漏洞，其中包括两个关于域权限提升的漏洞(CVE-2021-42278 和 CVE-2021-42287)。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。

- Microsoft Windows 10 拒绝服务漏洞 (CVE-2021-28312)

Windows 10，是由微软公司（Microsoft）开发的操作系统，应用于计算机和平板电脑等设备。2021 年 1 月 19 日，国外安全研究员称 Windows 10 存在未修复拒绝服务漏洞，通过浏览器等方式访问特定路径时，会立即导致系统崩溃并显示蓝屏。当开发人员想要直接与 Windows 设备进行交互时，可以将 Win32 设备的命名空间路径作为 Windows 编程功能的参数来进行传递。例如，应用程序直接与物理磁盘进行交互，而无需通过文件系统。当连接到该 Windows 设备时，开发人员应传递“ attach”扩展属性以确保与该设备进行正确通信。由于 Windows 10 系统的错误检查机制存在缺陷，导致可以尝试不通过该扩展属性直接连接到路径，则会导致异常，从而导致 Windows 10 系统崩溃。

- Sudo 本地权限提升漏洞 (CVE-2021-3156)

Sudo 是 linux 系统管理指令，通过 sudo 可以提高普通用户的操作权限，允许普通用户以系统管理者的身份执行执行 root 命令，大多数类 Unix 操作系统都包含 sudo。sudo 在 shell 模式下执行命令时，若带有-s 或-i 命令行选项，则会设置 MODE_SHELL 标志，之后 parse_args 函数会对输入进行校验，对特殊字符使用反斜杠转义，但当通过 sudoedit 运行-s 或-i 命令行选项时，实际上特殊字符没有被转义，从而可能导致缓冲区溢出，攻击者可使用本地普通用户权限在无密码的情况下利用此漏洞提升 root 权限。

- Windows TCP/IP 拒绝服务漏洞 (CVE-2021-24086)

2021 年 2 月 10 日，微软（Microsoft）发布了 2 月例行安全更新，其中包含 2 个 TCP/IP 高危漏洞的补丁，其漏洞编号分别为：CVE-2021-24074 和 CVE-2021-24086。Windows IPv6 协议栈存在一处拒绝服务漏洞，此漏洞的根本原因是 IPv6 的嵌套分片机制中，当尝试递归重组嵌套的分片时会计算内部有效载荷中包含的所有扩展标头，当重组扩展头约为 0xffff 字节的数据包时，在 IPv6 ReassembleDatagram 中发生的 NULL 指针取消引用，通过使用 Jumbograms 或者分片重组的方式可设置 Reassembly->UnfragmentableLength 为某个特殊值，从而引发空指针引用。远程攻击者可通过向目标系统发送特制数据包来利用此漏洞，成功利用此漏洞可导致目标系统拒绝服务（蓝屏）。

3.3 攻击态势分析

(1) 系统漏洞潜伏久，甚至可被蠕虫化利用，影响面扩大

随着网络安全的快速发展，其受重视程度也显著提高，攻击成功的难度加大，获取更多有价值的信息需要利用多个漏洞形成无差错攻击链，同时获得更高权限也十分重要。sudo 本地提权漏洞（CVE-2021-3156）潜藏了数十年，几乎所有基于 Unix 和 Linux 的操作系统都包含 sudo，攻击者可以在大多数*nix 系统中直接利用。Windows 系统中，攻击者可以通过 CVE-2021-34527 漏洞绕过安全验证，安装恶意的驱动程序。若攻击者所控制的用户在域中，可以使用一个低权限用户，对本地局域网中其他主机发起攻击，进一步控制存在漏洞的主机，若域控服务器被攻击成功，可控制整个网络，该漏洞存在于多个 Windows 版本中。

操作系统漏洞远程利用技术要求高，攻击难度相对复杂，潜在时间更长，受影响版本众多，提权类漏洞虽然可能无法直接被远程利用，但被成功利用后，可横向扩散，造成严重后果，在后渗透阶段起到至关重要的作用。

(2) 移动设备攻击面急剧扩大

随着 5G 技术的普及，生活、办公等业务逐渐迁移至移动端，直播、短视频等应用带来移动端设备用户的快速增长，移动设备攻击面也急剧扩大。根据 2021 年对操作系统的分类统计，移动设备操作系统漏洞占比 46.8%，如图 9 所示，众多知名厂商的操作系统爆发重大安全漏洞，影响全球数亿台设备。伴随着远程办公方式大规模兴起，企业组织也会遭受更多的移动端安全威胁，而各个用户的安全防护意识不相同，且相对终端设备，移动端设备难以统一管理，不能同步做到补丁升级，对于移动端的攻击会越来越复杂多样。

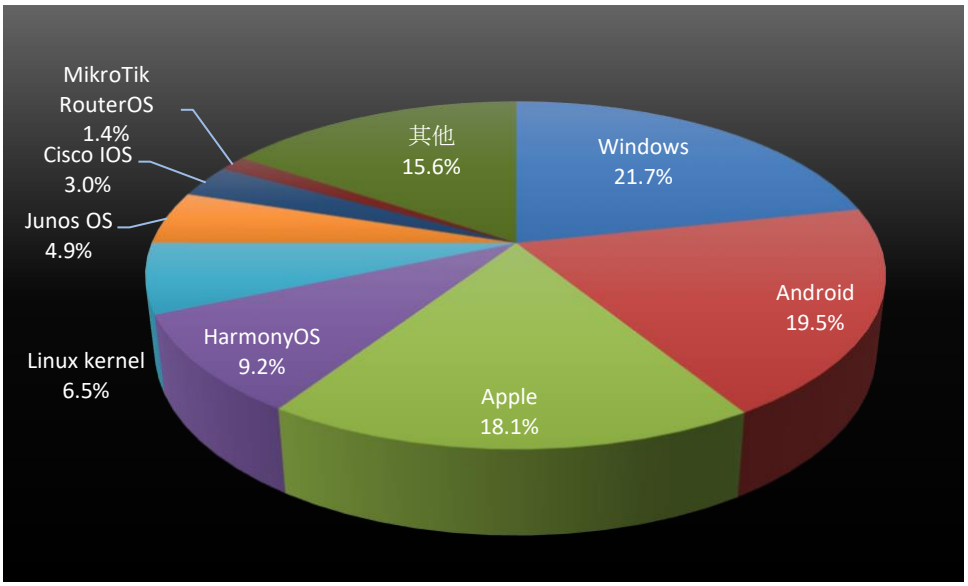

图 9 2021 年操作系统漏洞按系统分类占比

(3) Linux 成为针对 Windows 设备的潜在新攻击向量

Linux 在大多数网络中运行许多后端系统，但直到最近才在很大程度上被黑客社区所重视。Vermilion Strike 是臭名昭著的 Cobalt Strike 工具中关键功能 Beacon 的恶意实现。Cobalt Strike 是红队和威胁行为者用来证明网络破坏风险的“威胁模拟”软件程序，Beacon 旨在提供恶意负载，并在 Windows 环境中建立命令和控制(C2)连接。Vermilion Strike 以具有远程访问功能的 Linux 系统为目标，因为它在 Linux 环境中运行时完全不被检测到。

同时研究人员已检测到针对 Microsoft 的 Windows 下的 Linux 子系统(WSL)的新恶意二进制文件，WSL 是在 Windows 10、Windows 11 和 Windows Server 2019 上本地运行 Linux 二进制可执行文件的兼容层。2021 年该领域已经发生了一些变化，检测到的恶意测试文件充当加载程序，其中许多包含恶意负载。随着微软积极将 WSL 2 与 Windows 11 集成，使 Linux 成为针对 Windows 设备的潜在新攻击向量。

4 网络设备漏洞

路由器、防火墙、交换机等网络设备是整个互联网世界的联系纽带，占据着非常重要的地位，一旦控制网络设备，其连接的各种终端设备都将暴露在攻击者的面前，导致重要数据和资料泄漏，造成严重的网络安全事件。2021 年新华三共收录网络设备类漏洞 2665 条，较 2020 年同期（1912 条）增长 39.4%，对比 2020 年和 2021 年每月网络设备类漏洞变化趋势如图 10 所示。

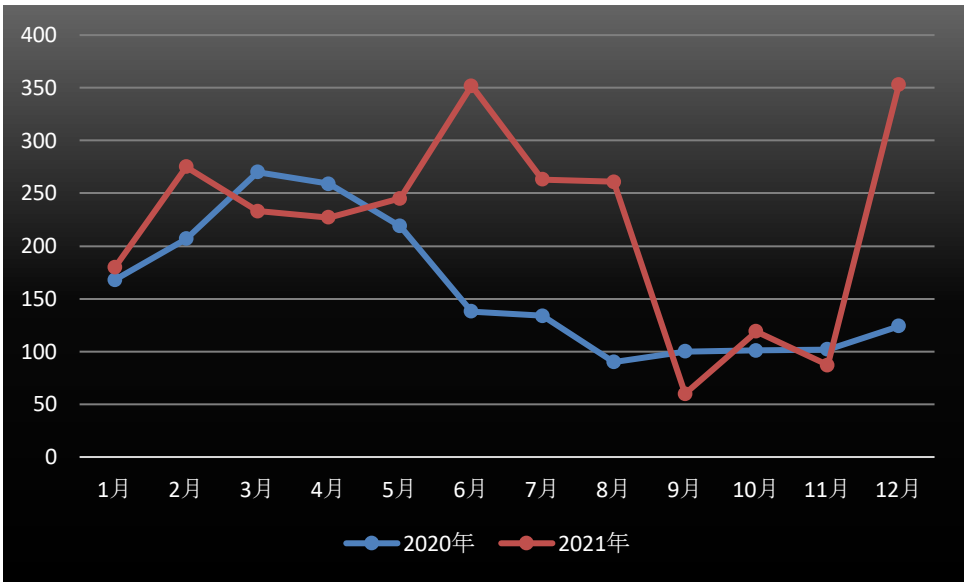

图 10 2020 与 2021 年网络设备新增漏洞趋势

5 漏洞分类

网络设备漏洞类型主要集中在弱口令、命令注入、缓冲区溢出、拒绝服务、授权问题等类型，如图 11 所示。大多数网络管理人员主要精力一般都集中于内部服务器、客户端、数据库的异常攻击行为，而对网络设备自身的安全性关注度并不足。而考虑到网络设备的性能，很多低端设备缺乏安全措施，出现漏洞后，可被直接利用。

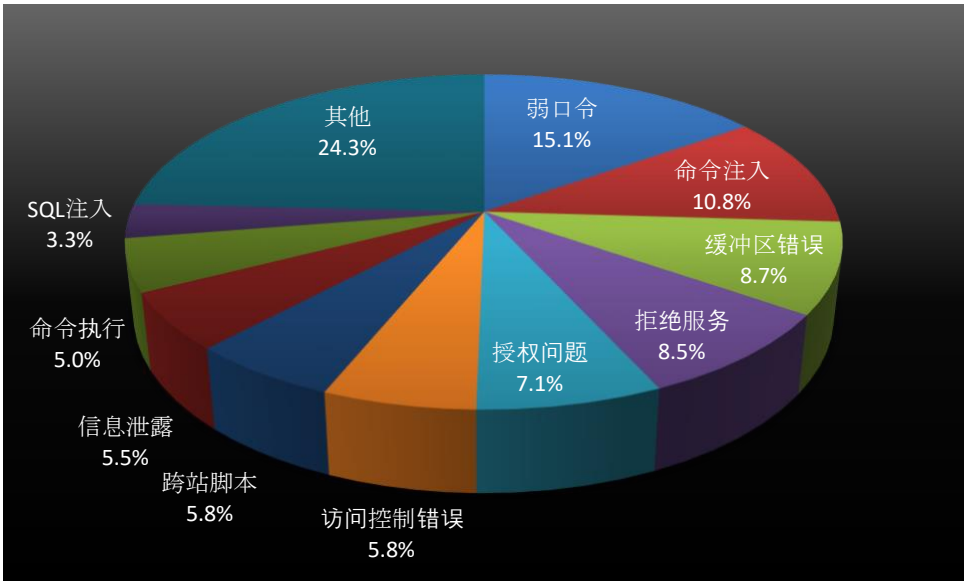

图 11 2021 年网络设备漏洞类型占比

5.1 重点漏洞回顾

漏洞名称	发布时间
Panabit Panalog cmdhandle.php后台命令执行漏洞	2021/1/15
Sonlogger任意文件上传漏洞(CVE-2021-27964)	2021/3/5
F5 BIG-IP iControl REST未授权远程代码执行漏洞(CVE-2021-22986)	2021/3/10
NETGEAR ProSAFE Network Management System路径遍历漏洞(CVE-2021-27275)	2021/3/26
Pulse Connect Secure远程代码执行漏洞（CVE-2021-22893）	2021/4/20
Cisco HyperFlex HX Data Platform 操作系统命令注入漏洞(CVE-2021-1498)	2021/5/6
CommScope Ruckus IoT Controller 任意读写漏洞	2021/5/27
Finetree 5MP Network Camera 未授权任意用户添加漏洞	2021/6/6
Hikvision Web Server命令注入漏洞(CVE-2021-36260)	2021/9/22
SonicWall SMA100路径遍历漏洞(CVE-2021-20034)	2021/9/24
TP-Link TL-WR840N 远程命令执行漏洞(CVE-2021-41653)	2021/11/13
NUUO Network Video Recorder 跨站脚本漏洞(CVE-2021-45812)	2021/12/28

经典漏洞盘点：

- JumpServer 远程代码执行漏洞

JumpServer 是全球首款开源的向企业级用户交付多云环境下的堡垒机，使用 Python / Django 编写，基于 ssh 协议来管理。与传统堡垒机相比，采用了业界领先的容器化部署方式，并且提供体验极佳的 Web Terminal ，还可实现基于 Web 的文件传输，并且支持用户将运维审计录像保存在云端。

2021 年 1 月，开源堡垒机 JumpServer 发布更新，修复一处未授权访问漏洞，该漏洞由于 JumpServer 某些接口未做授权限制，攻击者可构造恶意请求获取到日志等敏感信息，借此数据可生成认证 token，从而建立 websocket 连接，进一步执行任意命令。国内大量企业均采用此产品作为生产堡垒机，将超大规模的资产迁移至新平台，可见用户量巨大。由于该漏洞的利用门槛低且较容易被工具化，因此在发现后的很长一段时间内热度依旧很高。

- F5 BIG-IP 多个高危漏洞

2021 年 3 月 11 日，F5 官方发布安全通告，修复了影响 F5 的 BIG-IP 的多个高危漏洞（CVE-2021-22986，CVE-2021-22987，CVE-2021-22988，CVE-2021-22989），CVSS 评分均为 9.0 以上，建议相关用户采取措施进行防护。F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台，是当今使用的最受欢迎的网络产品之一，被广泛用于全球的政府网络，互联网服务提供商的网络，云计算数据中心内部以及整个企业网络中。

CVE-2021-22986，未经身份验证的恶意攻击者可以通过 BIG-IP 管理界面和自身 IP 地址对 iControl REST 接口发送恶意数据，从而能够远程执行任意系统命令，创建或删除文件以及禁用服务。

当 BIG-IP 以设备模式运行时，经过身份验证的攻击者可以使用控制界面利用 CVE-2021-22987 或 CVE-2021-22988，攻击者通过 BIG-IP 管理端口或自身 IP 访问 TMUI（Traffic Management User Interface，流量管理用户界面），进一步在目标机器上远程执行代码，创建或删除文件或禁用服务。

当在 BIG-IP 在设备模式下配置了 Advanced WAF 或 ASM 时，具有管理员、资源管理员或应用程序安全管理员角色权限的攻击者可以通过 BIG-IP 管理端口或自身 IP 地址访问 TMUI 从而利用 CVE-2021-22989，在目标服务器上执行任意系统命令，创建或删除文件，或禁用服务。

- Pulse Connect Secure 远程代码执行漏洞(CVE-2021-22893)

2021 年 04 月 20 日，PulseSecure 发布安全公告，公开了 Pulse Connect Secure（PCS）中的一个身份验证绕过漏洞（CVE-2021-22893），该漏洞的 CVSSv3 基本得分为 10.0 分。远程攻击可以通过利用此漏洞在 Pulse Connect Secure 网关上执行任意代码，且该漏洞无需经过身份验证即可利用。目前该漏洞在针对全球组织的攻击中已被积极利用，攻击者通过将 WebShell 放置在 Pulse Connect Secure 设备上，以实现进一步的访问和持久性。已知的 Webshell 具有包括身份验证绕过、多因素身份验证绕过、密码记录和持久性等多种功能。

5.2 攻击态势分析

(1) 安全意识不足，弱口令成为网络设备最大的安全隐患

随着数字化建设的快速推进，网络设备的数量也在快速增加，无论是路由器、防火墙、网关集成管理平台、VPN 还是 IDS、旁路流量监测产品，产品厂商生产后都会设置默认账号密码，而且权限一般都是管理员权限，能够执行服务器配置等重要信息。但是，由于大部分用户的安全意识不高或者其他原因，往往默认账号的密码并未进行修改或者修改后密码仍过于简单，攻击者通过弱口令字典

撞库，破解账号密码获得管理员权限。弱口令利用极其简单，危害又非常巨大，防御手段有限，而网络设备部署位置一般位于流量进出口，一旦被攻击者成功登录，造成的后果非常严重。

(2) 僵尸网络攻击目标逐渐转向网络设备，以快速扩大传播范围

网络产品作为物理设备连接到互联网的纽带，一旦被攻击者控制，将会造成极大的影响。近年来越来越多的网络设备被曝存在命令注入漏洞，比如今年下半年海康威视的多种产品就存在远程命令注入漏洞，僵尸网络家族利用命令注入漏洞向某些产品注入下载他们僵尸网络的命令，并通过网络设备的特性快速感染更多的网络设备，该僵尸网络曾经短短 12 小时就能感染 28 万的 IP，传播速度之快，范围之广由此可见。而由于低端路由器往往安全防御手段有限，在高端往上的设备才会有比较完整的安全防御措施，这也导致僵尸网络能够在家庭路由器等产品上快速蔓延，随之就是病毒软件下载或者数据信息泄露等，影响极大。

6 数据库漏洞

随着大数据的高速发展，各行业的数据量急速增长，数据库系统不可或缺，其存储了各类价值数据，已成为企业和组织重要的无形资产。与此同时，数据库也成为攻击者主要目标之一，一旦获得数据库权限，即可获得丰厚的利益。2021 年新华三收录数据库漏洞总数 285 条，相比 2020 年（266 条）大体持平，对比 2020 年和 2021 年每月数据库漏洞变化趋势如图 12 所示。

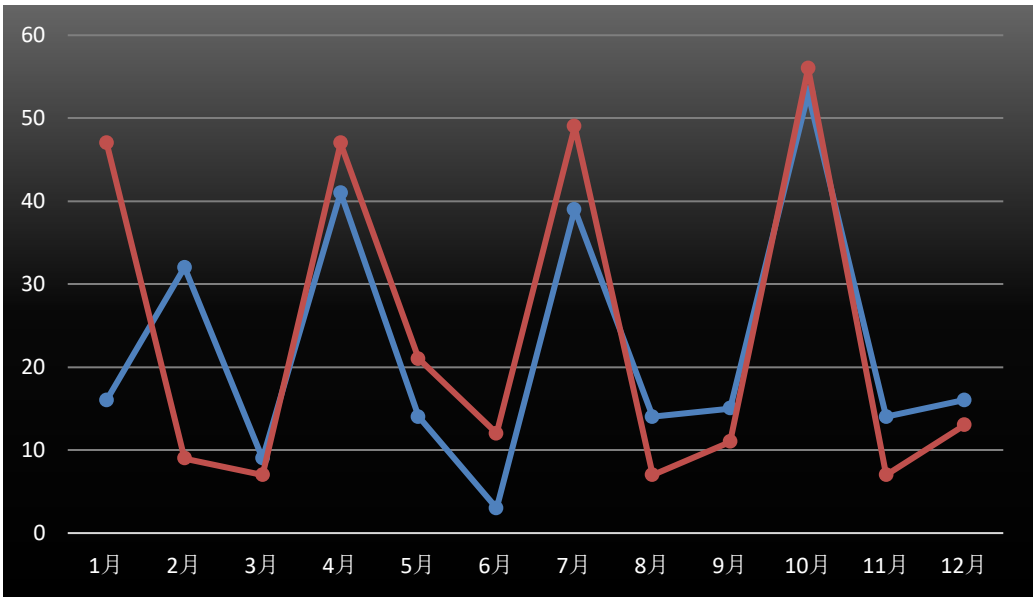

图 12 2020 与 2021 年数据库系统新增漏洞趋势

6.1 漏洞分类

MySQL 数据库由于代码开源、版本众多，加之使用量大，因此被发现的漏洞较多。2021 年被确认的 285 个数据库漏洞中，MySQL 漏洞 150 余个，占据总漏洞个数 55.1，如图 13 所示。

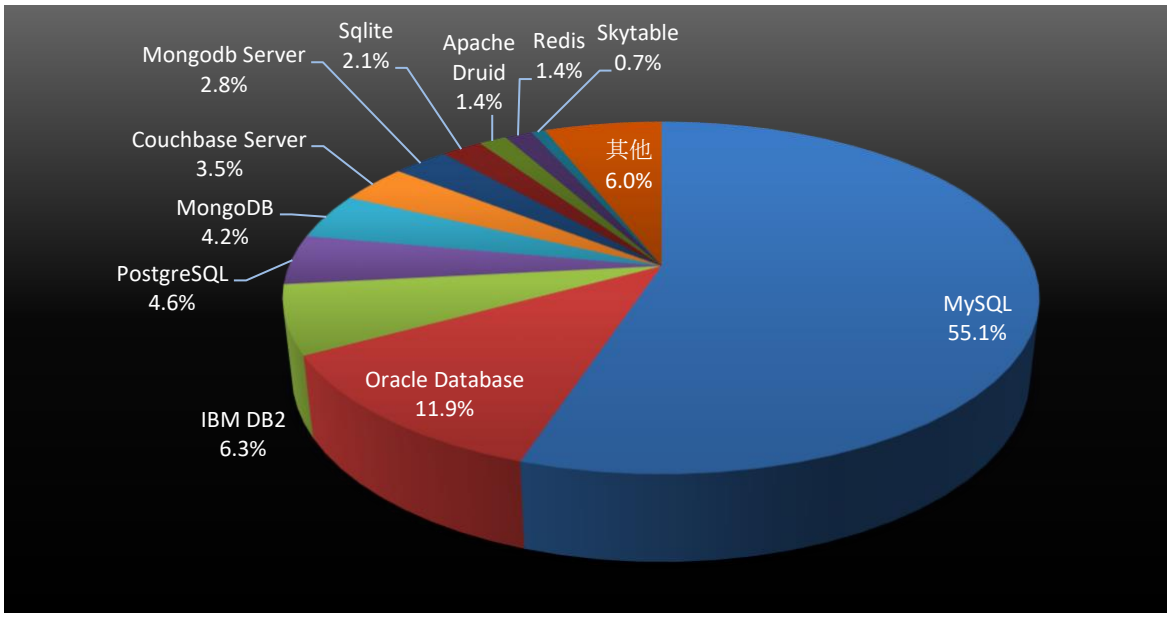

图 13 2021 年各数据库系统漏洞占比

从漏洞类型分布上来看，主要集中在输入验证错误、拒绝服务、访问控制错误三种类型，占据全部漏洞类型的 75.7%，如图 14 所示。

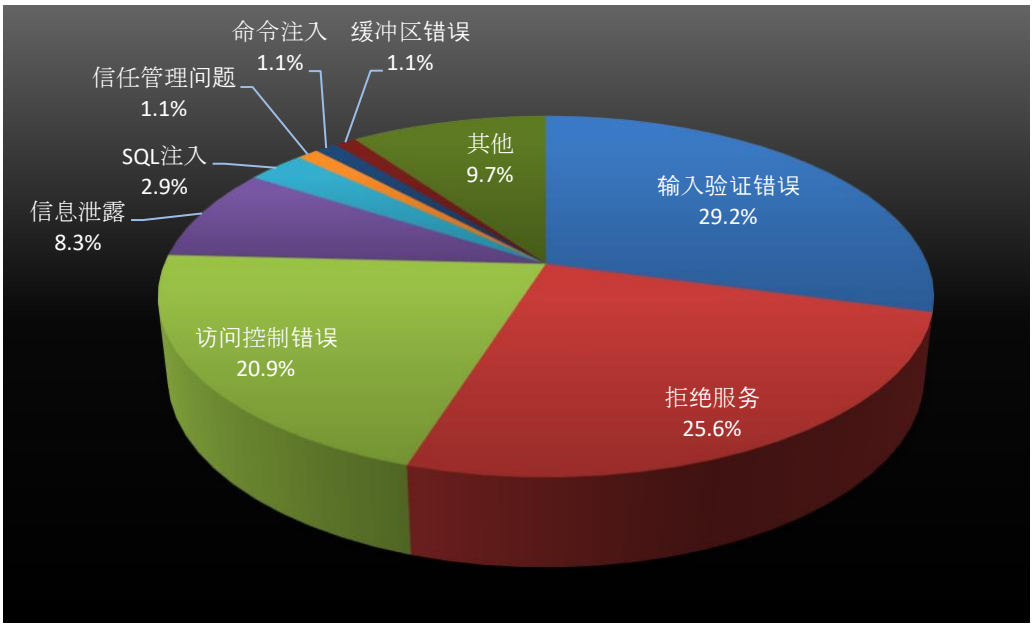

图 14 2021 年数据库漏洞类型占比

6.2 重点漏洞回顾

漏洞名称	发布时间
Apache_Druid远程代码执行漏洞(CVE-2021-25646)	2021/02/02

Oracle_MySQL_Server_输入验证错误漏洞(CVE-2021-2389)	2021/07/20
Redis远程代码执行漏洞(CVE-2021-32761)	2021/07/22
Neo4j基于RMI的远程代码执行漏洞(CVE-2021-34371)	2021/08/05
Apache_Druid任意文件读取漏洞(CVE-2021-36749)	2021/09/24

经典漏洞盘点：

- Oracle MySQL Server 输入验证错误漏洞(CVE-2021-2389)

Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。MySQL Server 5.7.34-8.0.25 版本存在输入验证错误漏洞，该漏洞源于 MySQL 的 InnoDB 组件内部输入验证不当导致的，远程未经身份验证的攻击者可利用该漏洞执行拒绝服务攻击。

- Redi 远程代码执行漏洞(CVE-2021-32761)

Redis 是美国 Redis Labs 公司的一套开源的使用 ANSI C 编写、支持网络、可基于内存亦可持久化的日志型、键值（Key-Value）存储数据库，并提供多种语言的 API。2021 年 7 月 22 日， Redis 发布安全公告，公开了 Redis 32 位系统上存在 Redis BITFIELD 命令整数溢出漏洞，通过修改默认的 proto-max-bulk-len 配置参数并构建特制的 bit 命令，攻击者可以破坏堆、泄漏任意堆内容或远程执行代码。

- Neo4j 基于 RMI 的远程代码执行漏洞(CVE-2021-34371)

Neo4j 是美国 Neo4j 公司的一款基于 Java 的且完全兼容 ACID 的图形数据库，它支持数据迁移、附加组件等。neo4j 存在代码问题漏洞，该漏洞源于任意反序列化 Java 对象的 RMI 服务。攻击者利用该漏洞可以造成远程代码执行。

- Apache_Druid 任意文件读取漏洞(CVE-2021-36749)

Apache Druid 是美国阿帕奇（Apache）基金会的一款使用 Java 语言编写的、面向列的开源分布式数据库。Apache Druid 0.22 之前版本存在安全漏洞，在 Druid ingestion system 中，InputSource 用于从某个数据源读取数据。由于没有对用户可控的 HTTP InputSource 进行限制，导致了 Apache Druid 允许经过身份验证的用户以 Druid 服务器进程的权限从其他来源读取数据，例如本地文件系统。攻击者可以通过将文件 URL 传递给 HTTP InputSource 来绕过应用程序级别的限制。由于 Apache Druid 默认缺乏授权认证，从而导致攻击者可以构造恶意数据利用该漏洞读取任意文件，最终导致服务器敏感信息泄漏。

6.3 攻击态势分析

(1) 云、AI、大数据背景下导致非关系型数据库漏洞利用方式显现

云、AI、大数据背景下使用非关系型数据库越来越多，像 NoSQL 数据库、Neo4j 数据库、基于文件的系统和 Hadoop 分布式等数据库，且越来越多有价值的数据库被迁移到分布式集群当中，这迫使供应商需要集成多个平台来满足日益复杂的场景。目前很少有供应商能为该环境提供全面的数据安全监控能力，从而导致该场景下的数据库可以利用的漏洞点突出；由于复杂环境和供应商的配套不及时从而导致了数据库的安全问题暴露出来，受到了攻击者的关注。

(2) 由于输入验证错误、访问控制错误导致的漏洞增多

公司、组织内疏忽大意的人通过粗心的行为将数据库暴露给攻击者，攻击者通过社会工程学或其他方法获取凭据或访问数据库，开发人员对用户输入验证不严格、特殊字符绕过未限制、配置不当、软件自身漏洞等方式都是攻击者常见的攻击数据库手段。

攻击者不断尝试利用数据库中软件、组件中的漏洞来突破防线拿下数据库服务，数据库管理软件和组件是攻击者非常容易攻击的有价值目标，开源数据库管理平台和商业数据库软件供应商都会定期发布安全补丁，但相关开发者不及时修复这些补丁，其数据库仍可能会被攻破。

7 工控系统漏洞

随着越来越多的工控系统暴露在互联网上，工控系统日益成为“众矢之的”，黑客有目的地探测并锁定攻击目标变得更加容易。加上针对工控系统的漏洞挖掘和发布与日俱增，大量工控系统安全漏洞、攻击方法可以通过互联网等多种公开或半公开渠道扩散，极易被黑客等不法分子获取利用。2021 年新华三收录的工控漏洞总数为 732 条，总数比 2020 年（645 条）增加 13.5%，对比 2020 年和 2021 年每月工控系统漏洞变化趋势如图 15 所示：

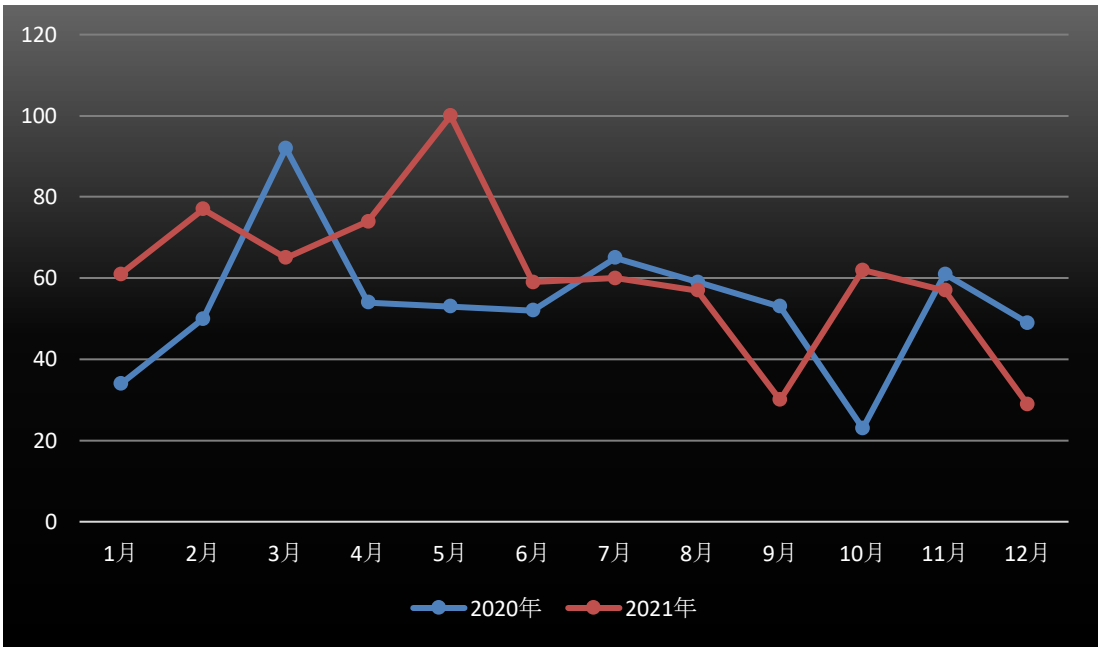

图 15 2020 与 2021 年工控系统新增漏洞趋势

7.1 漏洞分类

工控安全漏洞类型呈现出多样化特征，对于业务连续性、实时性要求高的工控系统，无论是利用这些漏洞造成业务中断、获得控制权限还是窃取敏感生产数据，都将对工控系统造成极大的安全威胁。工业企业最担心的严重后果是造成生产设备损坏、业务停滞，而拒绝服务漏洞排名一直靠前，如果被黑客利用，容易给企业造成较大影响。同时工控设备自身操作系统漏洞、应用软件漏洞及工业协

议的安全性缺陷等问题也不容忽视，根据统计，2021 年缓冲区错误、代码执行、SQL 注入等也是工控系统最为突出的问题，如图 16 所示。

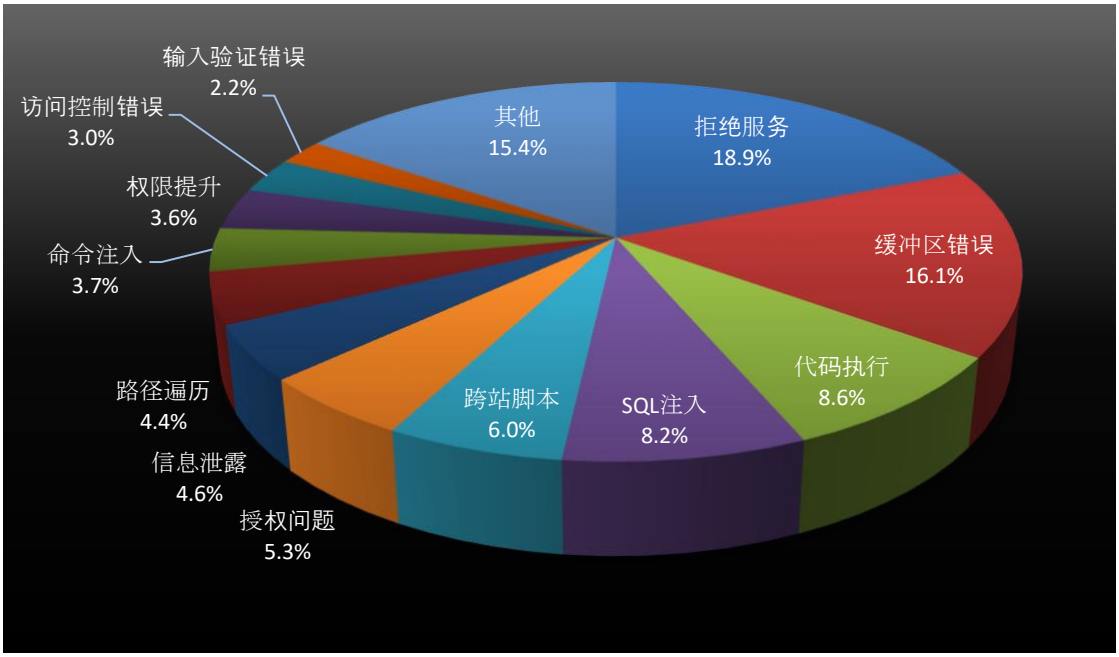

图 16 2021 年工控系统漏洞种类占比

7.2 重点漏洞回顾

漏洞名称	发布时间
Advantech iView远程代码执行漏洞(CVE-2021-22652)	2021/2/9
OpenPLC ScadaBR远程代码执行漏洞(CVE-2021-26828)	2021/5/13
Advantech R-SeeNet操作系统命令注入漏洞(CVE-2021-21805)	2021/7/15
Delta Electronics DIAEnergie SQL注入漏洞(CVE-2021-32983)	2021/8/26
Siemens SINEC NMS路径遍历漏洞(CVE-2021-37200)	2021/9/14

经典漏洞盘点：

- Advantech iView 远程代码执行漏洞(CVE-2021-22652)

Advantech Iview 是中国 Advantech 公司的一个基于简单网络协议（SNMP）来对 B + B SmartWorx 设备进行管理的软件。Advantech iView 中存在访问控制错误漏洞，该漏洞源于网络系统或产品未正确限制来自未授权角色的资源访问。

- OpenPLC ScadaBR 远程代码执行漏洞(CVE-2021-26828)

Sensorweb ScadaBR 是 Sensorweb 公司的一套用于开发自动化数据采集和监控应用程序的开源软件。ScadaBR 1.0 / 1.1CE 存在代码问题漏洞。该漏洞源于网络系统或产品缺乏有效的权限许可和访问控制措施。

- Advantech R-SeeNet 操作系统命令注入漏洞(CVE-2021-21805)

Advantech R-SeeNet 是中国台湾研华（Advantech）公司的一个工业监控软件。该软件基于 snmp 协议进行监控平台，并且适用于 Linux、Windows 平台。 Advantech R-SeeNet 存在操作系统命令注入漏洞，该漏洞源于 ping.php 的脚本功能。

- Delta Electronics DIAEnergie SQL 注入漏洞(CVE-2021-32983)

Delta Electronics DIAEnergie 是一个工业能源管理系统，用于实时监控和分析能源消耗、计算能源消耗和负载特性、优化设备性能、改进生产流程并最大限度地提高能源效率。 Delta Electronics DIAEnergie 存在 SQL 注入漏洞，该漏洞源于/DataHandler/HandlerEnergyType.ashx 端点中存在 SQL 盲注漏洞。攻击者可利用该漏洞在 NT SERVICEMSSQLSERVER 的上下文中执行任意代码。

7.3 攻击态势分析

(1) 工控攻击事件破坏性加剧，勒索为主要攻击手段

工控系统是公用事业工厂、工厂和其他设施的关键元素——它们被用于控制整个跨 IT-OT 网络的工业过程。如果勒索软件入侵了这些系统，它可能会持续对破坏数日之久，并增加关于设计、程序及其他敏感文件进入暗网的风险。勒索攻击赎金动辄高达数千万美金，使企业遭受了严重的经济损失，尤其是一些关键信息基础设施由于其自身的特殊性，在其遭受勒索攻击时，往往伴随着大范围的民生问题。从 Oldsmar 水利攻击事件导致水污染，到美国最大燃油管道 Colonial Pipeline 攻击事件导致多州进入紧急状态，及全球最大肉类加工企业 JBS FOODS 攻击事件导致其加工厂全球多地停产，工控系统一旦遭受攻击，影响面巨大，对国家安全、经济发展和社会稳定等产生了严重影响。

(2) 随着工控领域引入云平台，其安全风险类型更加复杂

工控行业本身具有覆盖企业多、业务场景杂、信息化基础设施弱的特点。伴随产业数字化的驱动，工控企业开始陆续引入工控云平台，建立工业物联网等方式，尝试进行数字化转型。其中，在数字化转型进程中启动较早，数字化工具引入较多的行业，相应的安全风险敞口也较为明显，如智能制造行业，能源行业，交通行业。此外，工业领域中业务场景广泛，企业安全技术水平参差不齐，导致攻击方式及安全威胁类型也多样，因此，工业企业更需要建设可定制化的专属解决方案。

8 云计算平台漏洞

云计算以其强大的弹性和高可拓展性，实现 IT 资源的规模效应最大化，云计算是数字时代的基础设施和智能引擎，云计算产业维持较高水平增长，与云计算相关的漏洞也逐年增长。2021 年新增云计算平台漏洞 1495 条，比 2020 年（总数 1316 条）增长 13.6%，近 2 年漏洞增长趋势如图 17 所示：

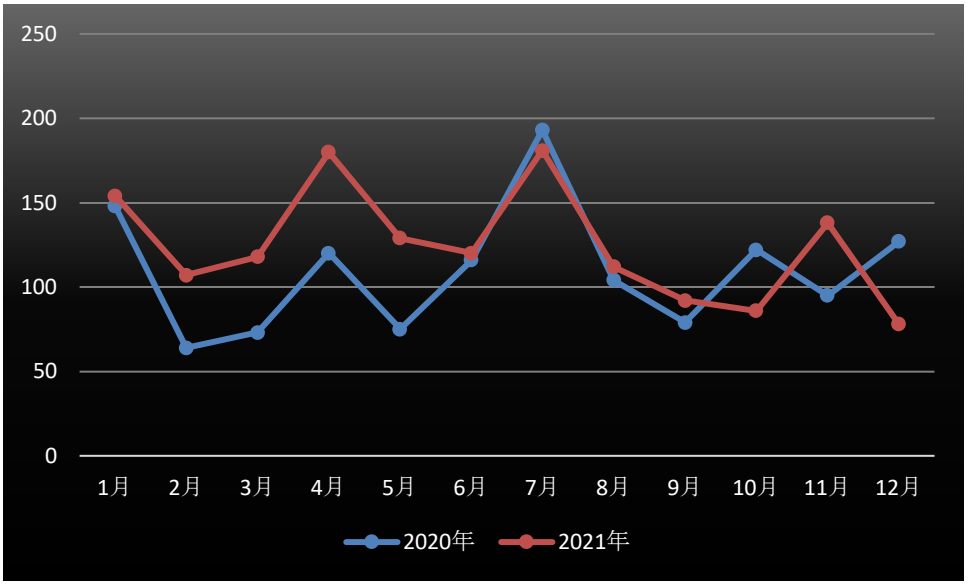

图 17 2020 与 2021 年云计算平台新增漏洞趋势

8.1 漏洞分类

伴随产业互联网发展，中国云计算行业整体迎来发展加速期，市场规模屡创新高，行业应用不断落地。伴随着云计算逐步成为数字经济的技术底座、企业数字化转型的关键基础设施，云计算所面对的潜在风险也显著提升。云计算能帮助企业提升业务敏捷性并降低成本，但同时也增加了攻击面。根据统计，其漏洞类型主要分布在权限许可和访问控制问题、信息泄露、输入验证错误等，如图 18 所示。

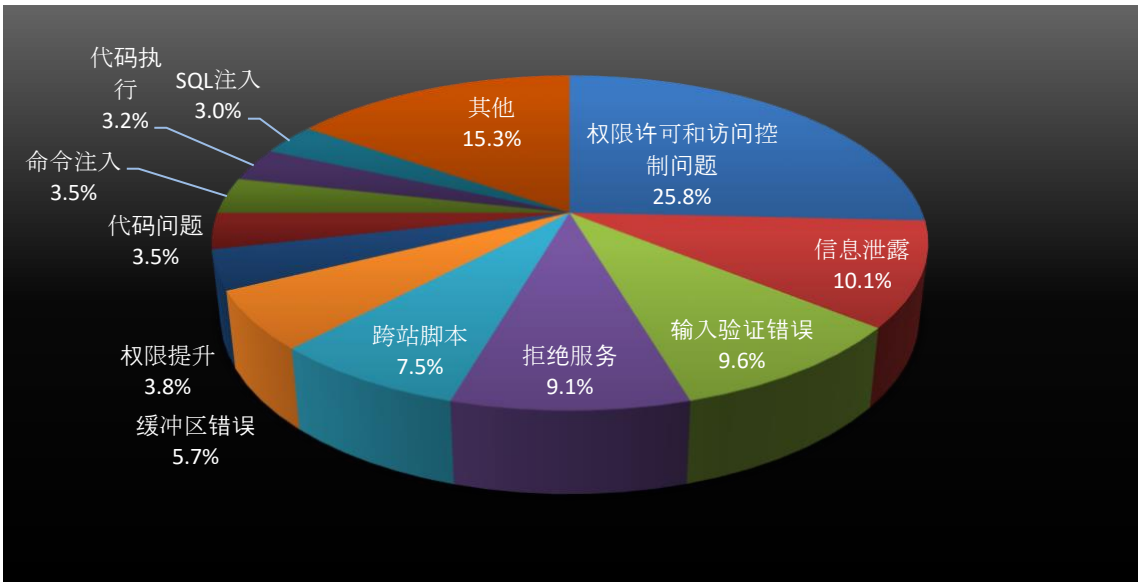

图 18 2021 年云计算平台漏洞类型占比

8.2 重点漏洞回顾

漏洞名称	发布时间
VMware vCenter Server服务端请求伪造漏洞(CVE-2021-21973)	2021/2/24
VMware ESXi OpenSLP堆缓冲区溢出漏洞(CVE-2021-21974)	2021/2/24
VMware View Planner远程代码执行漏洞(CVE-2021-21978)	2021/3/3
VMware vRealize Operations任意文件写入漏洞(CVE-2021-21983)	2021/3/31
Microsoft Hyper-V远程代码执行漏洞(CVE-2021-28476)	2021/5/11
Apache Pulsar JSON Web Token认证绕过漏洞(CVE-2021-22160)	2021/5/25
VMware vCenter远程代码执行漏洞(CVE-2021-21985)	2021/5/26
Microsoft Azure Open Management远程代码执行漏洞(CVE-2021-38647)	2021/9/14
VMware vCenter Server任意文件上传漏洞(CVE-2021-22005)	2021/9/21
Apache Hadoop Yarn RPC未授权访问漏洞	2021/11/15
VMware Spring Cloud Netflix 模板解析漏洞(CVE-2021-22053)	2021/11/19
Docker操作系统命令注入漏洞(CVE-2021-23732)	2021/11/22

经典漏洞盘点：

- Apache Hadoop Yarn RPC 未授权访问漏洞

Hadoop 是一个由 Apache 基金会所开发的分布式系统基础架构，RPC（Remote Procedure Call）即远程过程调用，是所有分布式系统的基础。该漏洞是由于 Hadoop Yarn 默认开放 RPC 服务且不需要身份验证，恶意攻击者可以通过编写 Yarn Client，在未授权的情况下向 Apache Hadoop Yarn RPC Serve 提交 Application，从而利用 Hadoop 的 RPC 服务执行任意命令，最终控制服务器。此外，由于 Hadoop Yarn RPC 服务的访问控制机制开启方式与 REST API 不一样，所以即使在 REST API 有授权认证的情况下，RPC 服务所在端口仍然可以未授权访问。2021 年 11 月 15 日，Hadoop Yarn RPC 未授权访问漏洞被监测到在野利用，用于大规模蠕虫传播和挖矿勒索。

- VirtualBox 权限提升漏洞

2021 年 11 月 23 日，国外安全研究人员公开了 Oracle VirtualBox NAT 权限提升漏洞（CVE-2021-2310）、Oracle VirtualBox NAT 权限提升漏洞（CVE-2021-2145）和 Oracle VirtualBox NAT 拒绝服务攻击漏洞（CVE-2021-2442）的技术细节，Oracle VirtualBox 是一款功能强大的 x86 和 AMD64/Intel64 虚拟化产品，适用于企业和家庭使用。经过身份验证的攻击者可以利用 Oracle VirtualBox NAT 权限提升漏洞进行权限提升，将普通权限提升为 root 权限。远程的攻击者可以利用 Oracle VirtualBox NAT 拒绝服务攻击漏洞对目标机器进行拒绝服务攻击，使目标机器宕机。

- VMware View Planner 远程代码执行漏洞 (CVE-2021-21978)

View Planner 是 VMware 官方推出的一款针对 view 桌面的测试工具，通过这个测试工具可以估算出在指定的应用环境下可以发布多少个 view 桌面。2021 年 03 月 04 日，VMware 发布了 View Planner 的风险通告，漏洞编号为 CVE-2021-21978，严重等级为高危，评分 8.6。View Planner logupload 的 web 上传接口没有正确的对 itrLogPath 参数进行输入校验且缺乏授权，View Planner 会获取 itrLogPath 和 logFileType 的值，并将 itrLogPath 和 logFileType 与 resultBasePath 进行路径拼接，导致未经授权的攻击者可以通过构造参数实现目录穿越并上传文件至任意目录，从而覆盖 log_upload_wsgi.py 文件，达到远程代码执行的目的。

- Docker 操作系统命令注入漏洞(CVE-2021-23732)

Docker 是美国 Docker 公司的一款开源的应用容器引擎。该产品支持在 Linux 系统上创建一个容器（轻量级虚拟机）并部署和运行应用程序，以及通过配置文件实现应用程序的自动化安装、部署和升级。 docker cli-js 存在操作系统命令注入漏洞，该漏洞源于如果 Docker.command 方法的 command 参数至少可以由用户部分控制，他们将能够在主机系统上执行任意操作系统命令。

- Microsoft_Hyper-V 远程代码执行漏洞(CVE-2021-28476)

Microsoft Hyper-V 是美国微软（Microsoft）公司的一个应用程序，用于在 Windows 系统和 Azure 云计算环境中创建虚拟机的本机管理程序。2021 年 5 月 11 日，微软发布 Microsoft Hyper-V 远程代码执行漏洞安全通告，CVE-2021-28476，并发布了修复补丁。2021 年 6 月 1 日，国外安全研究人员公开了 Microsoft Hyper-V 远程代码执行漏洞的技术细节和 PoC。经过身份认证的攻击者可以利用该漏洞使 host 主机奔溃或者在 host 主机上执行任意代码，一台云环境下的主机收到该漏洞攻击会影响到整个云环境下的所有主机。

8.3 攻击态势分析

(1) 云原生安全逐步成为云基础安全重点

伴随云原生应用下沉，云原生安全逐步成为云基础安全重点。云原生技术经过长足发展，已逐步被广泛应用，并逐步突破容器、微服务、DevOps 等领域，开始形成更完整的云原生产品架构，云原生的应用在显著提升云计算产品能力的同时，也带来的更为复杂的安全需求。传统的安全防护理念，“非原生化”的安全产品与服务均不能满足云原生安全需求。为保障云原生安全，需要更深刻理解云原生架构，熟悉云原生特点，针对云原生不同产品特性，提供针对性安全对策，并从下至上构建完整解决方案。

(2) 安全基线风险日益凸显，云上业务存在高危风险

安全基线检测数据显示，云上资产安全现状不容乐观，主要为口令过期后账号最长有效天数策略、帐户超时自动登出配置和限制 root 权限用户远程登录等。安全基线检测能有效提高入侵门槛，容易被安全运维人员忽略而成为黑客利用的漏洞，需要严格按照安全规范配置，符合国家等保合规要求。高危命令有可能是黑客入侵之后执行的命令，以企图控制主机甚至破坏系统，也有可能是运维人员在日常操作时候执行的风险命令。数据显示云上业务主要的高危命令有设置操作命令不记录进日志、nc 命令执行和 wget 下载后执行命令等。即使高危命令并非攻击者执行，但过于频繁执行高危命令，意味着可能存在安全管理疏忽大意、权限管理不够严谨等风险，需要企业 IT 负责人警惕。

9 总结与建议

9.1 总结

2021 年对比 2020 年，网络安全漏洞数量和网络攻击数量都有增长，网络威胁与攻击始终在不断变化，其攻击目的更直接地盯上客户的业务相关的数据等，一旦成功，不仅是对客户业务本身造成影响，这些泄露的数据也会成为获利的手段，被拿下的服务器可能会成为挖矿或者攻击其他目标的资源，对企业造成更长久的损害。

Web 类针对高危漏洞的入侵依然以组件漏洞为主，应用组件漏洞比操作系统漏洞具备更容易获得的执行环境，比业务漏洞具有更强的通用性，通常黑产团队会选择用户数量较多、漏洞利用条件简单且稳定的漏洞来开发自动化工具，以较低的成本实现对目标的控制、自动化挖矿等牟利行为；操作系统类漏洞以缓冲区溢出与权限提升为主，操作系统类漏洞影响面大，利用成功容易爆发蠕虫病毒传播事件与勒索事件；网络设备类漏洞大幅增加，网络设备由于漏洞被攻击的事件越发频繁，弱口令占比高居不下，用户安全意识仍需提高；工业互联网作为关键技术设施，遭遇勒索攻击赎金动辄高达数千万美金，使企业遭受了严重的经济损失，同时往往伴随着大范围的民生问题；在云计算生态环境下，云原生所依赖的容器、微服务等技术在提升业务的敏捷性的同时，也引入了新的安全风险，比如容器逃逸风险、镜像安全风险等，同样可直接损害业务运行、造成业务数据失窃。

从攻击手段上看，黑客攻击已呈现出自动化程度提升、隐蔽性增强的特点，用 AI 模拟人行为绕过常规安全规则匹配的手段屡见不鲜，入侵检测和防护的难度水涨船高。在这一趋势下，企业在提供线上服务时需要认真考虑从网络层到应用层的综合性安全防护方案，形成纵深防御，阻止攻击者触及核心业务应用和数据，造成损失。

9.2 安全建议

在漏洞态势不断发生变化的大环境中，新华三秉承维护计算机网络空间安全的核心理念，从漏洞的视角针对目前的安全建设提出一些建议。对于安全建设有一些公共安全建议，例如及时安装系统和软件的更新补丁，隔离办公网和生产环境，主机进行集成化管理，配置防护系统实时在网络传输层进行链路阻断，禁止外部 IP 访问特殊端口（如 139、445、3389 端口），采用最小化端口与服务暴露原则等。对于各个不同分类漏洞，安全建议不尽相同，具体如下：

(1) Web 应用安全建议

Web 类应用系统的应用软件需要具备一定的安全功能，来保证系统本身不被攻击或破坏。能够通过某种形式的身份验证来识别用户，并确保身份验证过程是安全的。为了防止一些恶意输入，还要对输入的数据和参数进行校验。另外还要考虑 Web 系统的安全配置、敏感数据的保护、用户的权限管理以及所有操作的安全审计。因此 Web 应用系统本身安全建议如下：

- 身份验证：管理页面采取强口令策略。系统登录验证口令具备一定的复杂度。网页上的登录、认证表单加入强身份认证机制，如验证码、动态口令卡等。对于常见的敏感帐号，如：root、admin、administrator 等，在系统安装完成之后修改为其它名称或者禁用。
- 会话管理：会话过程中不允许修改的信息，作为会话状态的一部分在服务器端存储和维护。不通过隐藏域或 URL 重写等不安全的方式存储和维护。不使用客户端提交的未经审

核的信息来给会话信息赋值，防止会话信息被篡改。用户登录后分配新的会话标识，不能继续使用用户未登录前所使用的标识。

- 权限管理：用户权限最小化和职责分离。一个帐号只能拥有必需的角色和必需的权限。授权和用户角色数据存放在服务器端，鉴权处理也在服务器端完成。不将授权和角色数据存放在客户端中（比如 Cookie 或隐藏域中），以防止被篡改。拒绝用户访问 Web 服务器上不公开的内容，应对各种形式执行程序的访问进行控制。
- 敏感数据保护：敏感数据（比如密码、密钥等）加密存储、加密传输。隐藏域中不存放明文形式的敏感数据。采用安全的密码算法对敏感信息进行加密。
- 程序设计：不在程序中将密码、密钥等数据固化，不在代码中存储如数据库连接字符串、口令和密钥之类的敏感数据。
- 安全审计：对于业务运行异常、非法访问、非法篡改等异常行为应有完整的记录，包括事件的源 IP、事件的类型、事件发生的动作、事件时间等。
- 代码安全：在开发过程中，注意代码安全，主要包括对 SQL 注入、用户输入脚本过滤、Cookie 管理、信息泄露等常见威胁的预防。在代码注释信息中禁止包含数据库连接信息、SQL 语句信息。
- 中间件安全：中间件版本、安全补丁及时更新，加强安全配置、安全加固，避免被黑客等利用攻击整个系统。

(2) 操作系统安全建议

操作系统是运行应用程序的物理环境，操作系统中的任何漏洞可危害应用程序的安全性。通过保护操作系统安全，可以使环境稳定，控制资源的访问，以及控制环境的外部访问。

针对操作系统的安全策略和建议如下：

- 用户帐户策略：限制服务器计算机上的用户帐户数，减少不必要的和旧的用户帐户；确保仅一些可信用户具有对服务器计算机的管理访问权限，为运行应用程序的帐户分配所需的最低访问权限。
- 密码策略：开发和管理操作系统安全的密码策略，采用高强度密码规则。
- 文件系统策略：为用户授予所需目录的只读权限，缺省情况下，拒绝访问权限，除了被明确授予访问权限的用户，拒绝所有人对资源的访问。
- 网络服务策略：仅使用运行应用程序所需的服务，例如，可能不需要 FTP、Rlogin 或 SSH 服务；为网络服务用户减少访问权限的级别；确保具有 Web 服务器访问权限的用户帐户不可访问 shell 功能；确保未使用的服务没有运行，且它们没有在操作系统上自动启动；删除或注释掉未计划使用的端口，减少系统的可能入口点；保护系统免受与端口 137、138 和 139 相关联的 NetBIOS 威胁。
- 系统补丁策略：经常检查安全性更新，确保服务是最新的；为操作系统运行供应商建议的最新补丁。
- 操作系统最小化：除去不重要的应用程序来减少可能的系统漏洞。
- 记录和监控策略：记录安全性相关的事件，包括成功和失败的登录、注销和用户权限的更改；监视系统日志文件，通过限制对系统日志文件的访问权限，保护其安全；保护维护日志免受篡改；保护日志记录配置文件的安全。
- 定期备份系统资源。

（3）网络设备安全建议

网络设备在网络中处于重要位置，网络安全产品属于企业边界防护的关键设施，当其产品出现漏洞时，将会对企业造成非常严重的安全威胁。

对于企业用户安全建议：

- 在购置设备前应对产品进行安全测试；
- 在部署时应严格设置设备的访问控制权限，避免当设备沦陷时攻击者获得较高权限访问敏感网段；
- 在设备运行时做好访问权限控制（如 IP 限制等），关闭不需要的服务；
- 在运营设备时应同样对设备进行日志记录和审计；
- 当漏洞出现时，及时联系厂商进行设备的更新及售后。

对于厂商安全建议：

- 在产品发布前应对产品进行严格的安全测试；
- 及时关注最新的安全技术，及时修补产品中存在漏洞的第三方库等外部依赖。

(3) 数据库安全建议

数据库软件漏洞属于产品自身的缺陷，由数据库厂商对其修复，通常以产品补丁的形式出现。针对数据库漏洞攻击的数据库加固方式可以采用购买第三方产品，安全建议如下：

- 采取用户权限最小化原则，配置数据库帐号时，满足应用系统使用的最小权限的账号，任何额外的权限都可能是潜在的攻击点。
- 定期安装数据库厂商提供的漏洞补丁，即使由于各种原因无法及时打补丁，通过虚拟补丁等技术暂时或永久加固数据库。
- 对数据库进行安全配置，数据库默认安装下并不会开启所有安全配置，在充分考虑对应用的影响后，尽可能开启数据库自身提供的安全设置将会极大降低被不法分子攻击的成功率。
- 采取数据库功能最小化原则，对于用户来说，大部分数据库功能组件根本不会使用。在综合应用和运维后，划定一个使用组件的最小范围。删除数据库中不用的组件，减少数据库组件可以有效的减少用户面对的风险面。
- 配置高强度密码，杜绝弱口令或默认口令。

(4) 工控系统安全建议

一般现代工业控制系统多由以下几个关键部分组成：人机界面 HMI，远程终端单元 RTU，综合监管系统和可编程逻辑控制器 PLC。由上述部分组成的工业控制系统主要有以下几个风险点：病毒容易通过企业办公网感染综合监管系统，工控系统中多余的 USB 接口封闭不足，对远程维护通道未加严格限制，导致生产网直接暴露在互联网上。

因此，建议执行以下操作来加强工控系统运行安全：

- 分离工业控制系统的开发、测试和生产环境。
- 通过工业控制网络边界防护设备对工业控制网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的工业控制网络与互联网连接。严格限制工业控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务。
- 通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离安全防护，在重要工业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。

- 拆除或封闭工业主机上不必要的 USB、光驱、无线等接口，若确需使用，通过主机外设安全管理技术手段实施严格访问控制。
- 在工业主机登录、应用服务资源访问、工业云平台访问等过程中使用身份认证管理，对于关键设备、系统和平台的访问采用多因素认证。
- 合理分类设置账户权限，以最小特权原则分配账户权限。
- 强化工业控制设备、SCADA 软件、工业通信设备等的登录账户及密码，避免使用默认口令或弱口令，定期更新口令。
- 对远程访问采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，并采用加标锁定策略，远程维护采用虚拟专用网络（VPN）等远程接入方式进行。
- 在工业控制网络部署网络安全监测设备，及时发现处理网络攻击或异常行为，在重要工业控制设备前端部署具备工业协议深度包检测功能的防护设备，限制违法操作。
- 保留工业控制系统的相关访问日志，并对操作过程进行安全审计。

(5) 云计算安全建议

云计算基于虚拟化和分布式计算技术，云计算服务已经不单单是一种分布式计算，而是分布式计算、效用计算、负载均衡、并行计算、网络存储、热备份冗杂和虚拟化等计算机技术混合演进并跃升的结果。云计算技术正在不断改变组织使用、存储和共享数据、应用程序以及工作负载的方式，与此同时，它也引发了一系列新的安全威胁和挑战。云计算安全包括操作系统安全、数据安全、应用安全、网络控制安全等，对其安全建议如下：

云服务提供侧：

对于云服务商，需要构建安全稳定的基础设施平台，并且面向应用从构建、部署到运行时刻的全生命周期构建对应的安全防护手段：

- 云平台基础设施层的安全：基础设施主要包括支撑云服务的物理环境，以及运维运营包括计算、存储、网络、数据库、平台、应用、身份管理和高级安全服务等各项云服务的系统设施。云平台基础设施层是保障业务应用正常运行的关键，云服务商需要确保各项云技术的安全开发、配置和部署安全。
- 云服务的自身安全配置和版本维护：建立版本更新和漏洞应急响应机制，虚机 OS 的版本更新和漏洞补丁的安装能力也是保证基础设施安全的基本防护措施，除此之外如 K8s 等容器相关开源社区的风险漏洞，都可能成为恶意攻击者首选的攻击路径，需要厂商提供漏洞的分级响应机制并提供必要的版本升级能力。
- 平台的安全合规性：云服务商需要基于业界通用的安全合规标准，保证服务组件配置的默认安全性，同时面向平台用户和安全审计人员，提供完备的审计机制。
- 业务应用侧提供纵深防御能力：云服务商提供适合云场景下应用的安全防护手段，帮助终端用户在应用生命周期各阶段都能有对应的安全治理方案。

企业安全侧：

对于企业的安全管理和运维人员来说，首先需要理解云上安全的责任共担模型边界，究竟企业自身需要承担起哪些安全责任。对于企业安全管理人员来说可以参考关注如下方向加固企业应用生命周期中的生产安全：

- 应用制品的供应链安全：对于企业来说制品供应链环节的安全性是企业应用生产安全的源头，一方面需要在应用构建阶段保证制品的安全性；另一方面需要在制品入库，分发和部署时刻建立对应的访问控制，安全扫描、审计和准入校验机制，保证制品源头的安全性。
- 权限配置和凭证下发遵循权限最小化原则：对于企业安全管理人员来说，需要利用云服务商提供的访问控制能力，结合企业内部的权限账号体系，严格遵循权限最小化原则配置对云上资源的访问控制策略；另外严格控制资源访问凭证的下发，对于可能造成越权攻击行为的已下发凭证要及时吊销。
- 关注应用数据和应用运行时刻安全：除了配置完备的资源请求审计外，安全管理运维人员还需要保持对应用运行时安全的关注，及时发现安全攻击事件和可能的安全隐患。
- 及时修复安全漏洞和进行版本更新：无论是虚机系统，容器镜像或是平台自身的安全漏洞，都有可能被恶意攻击者利用成为入侵应用内部的跳板，企业安全管理运维人员需要根据云服务商推荐的指导方案进行安全漏洞的修复和版本更新。

10 结语

2021 年，国际环境日趋复杂，全球产业链、供应链遭受冲击，网络空间安全面临的形势持续复杂多变。网络空间对抗趋势更加突出，大规模针对性网络攻击行为增加，安全漏洞、数据泄露、网络诈骗等风险增加。世界主要国家和地区不断推出关键信息基础设施保护、供应链安全、数据安全、个人信息保护等方面法规和政策，平台反垄断监管不断强化。网络安全企业积极探索以网络弹性技术为代表的网络风险防范能力、以安全多方计算为代表的数据隐私保护技术等。面对日益增长的网络信息安全威胁，新华三会持续引入新兴技术研究成果，加强威胁漏洞情报积累，形成更加及时、精准有效、覆盖全面的网络空间安全态势感知体系，提升网络安全防护水平。