奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

关键词：关键漏洞、在野利用、年度安全大事件、漏洞情报、APT

2021年度
漏洞态势观察报告

——兼谈我们需要什么样的漏洞情报

奇安信安全监测与响应中心

核心洞见 Opinions

在数字的世界里，安全是一个永恒的话题。回顾刚刚过去的 2021 年，安全事件频发，网络攻击愈演愈烈，2021 年第二季度网络攻击量达到 2018 年初以来最高值。一方面，安全研究人员规模在不断扩大，不断挖掘和修复新的安全漏洞维护网络安全；另一方面，随着厂商安全性的提高，及时分发补丁策略，黑客组织不惜使用 0day 漏洞发起攻击。网络空间的战场看不见硝烟，却和我们的生活越来越息息相关，开源应用安全、云安全、供应链安全……越来越多的受到大家关注。

《奇安信 CERT——2021 年度漏洞态势观察报告》围绕漏洞监测、漏洞分析与研判、漏洞情报获取、漏洞风险处置等方面描绘过去一年全网漏洞态势，并对 2021 年度有现实威胁的漏洞进行重点分析和回顾。思考在漏洞造成实际危害前，对于个人、企业以及漏洞情报供应商而言，可以采取哪些措施来有效隔离风险。基于我们所收集到的事实，本报告的主要洞见如下：

1. 尽管存在对应 Exploit（漏洞利用代码或工具）的漏洞占到了总漏洞数的 22.06%，但其中的大部分并未监测到实际利用的发生，漏洞是否真的被利用，还取决于漏洞的可达性、利用条件和危害程度。从公开信息来看，**实际存在野外利用的漏洞，仅占漏洞总量的 1 %~2 %左右。**所以，**基于威胁情报的漏洞处理优先级排序对于威胁的消除将起到事半功倍的效果。**

2. 另一方面看漏洞的利用，已知存在野外利用的漏洞有 46%也就是一小半左右并没有公开的漏洞 Exploit，这个事实暗示了**一大部分漏洞的威胁并没有显式的呈现，攻击面的削减管理也非常重要。**

3. 2021 年的攻防演习期间大量的 0day 漏洞被使用，其中很大部分为国外漏洞库并不收录的国产软件漏洞，这些漏洞如果被国家级的对手利用将导致非常严重的后果。**事实上我们看到的活跃国外 APT 组织已经在这样做了，提示了国内挖掘自己特有软件漏洞并共享情报的高度必要性。**

4. **明星漏洞存在很强的聚光灯效应，当某个软件出现重大漏洞时会引起超高关**

注度的产品极易在未来一段时间出现更多漏洞，如：Apache Log4j 连续被曝 4 个远程代码执行漏洞、Microsoft Exchange Server 在被曝出 ProxyLogon 漏洞之后又出现了 ProxyShell 等漏洞。但是，**由于明星漏洞衍生出来的新漏洞大概率未必有同等的威胁和影响面，需要漏洞情报分析运营团队进行深入的研判确认其利用真正的威胁**，非常考验团队的响应能力。

5. 由于多种技术层面以外因素的影响，相同 CVSS 评分的漏洞所能导致实际安全风险往往天差地别，**结合情报的导致影响威胁升级的关键因素监测，确认漏洞对于风险的影响才具备了真正的动态性**。

6. 有效的漏洞情报可以帮助用户快速、准确、全面的定位资产相关的漏洞风险，在详细多角度的处理方案的建议下实现相应威胁的消除和缓解。基于漏洞对不同类型用户的影响和处理要求，个人用户、企业用户以及安全监管单位在漏洞情报的选择上应遵循**“C 端用户挑产品、B 端用户挑服务、监管机构挑供应商”的原则。**

目录 Contents

1. 2021年度漏洞态势

1.1 年度漏洞处置情况

2021 年 NVD（美国国家漏洞库）每月新增漏洞信息条数如图 1-1 所示：

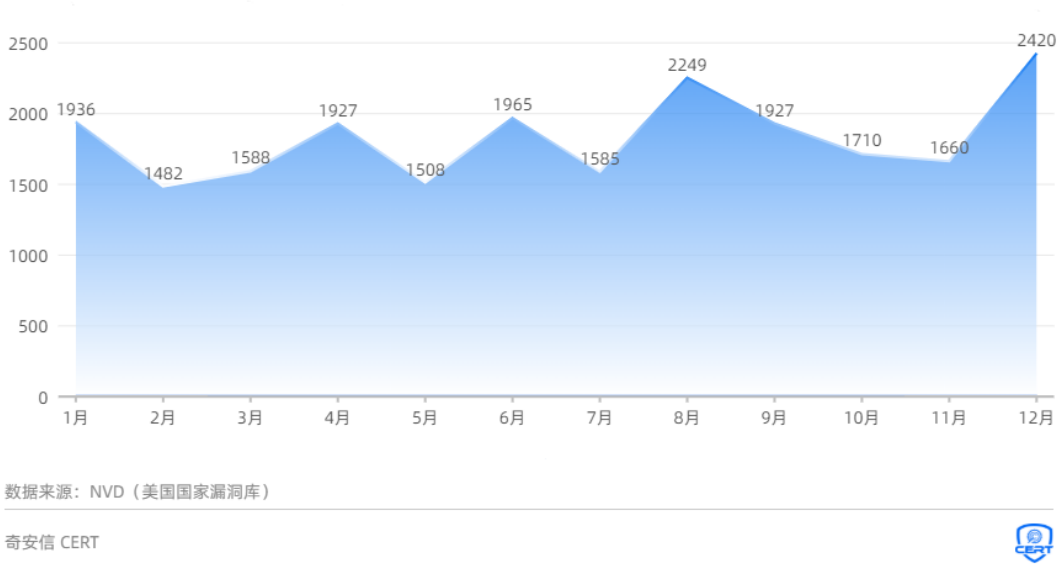

图 1-1 2021 年每月新增漏洞信息数量

2021 年全年 NVD 共发布 CVE 漏洞信息 21,957 条，其中有详细信息的漏洞有 20,791 个，无详细信息的漏洞有 1,166 个（占漏洞总条目的 5.31%），如图 1-2 所示：

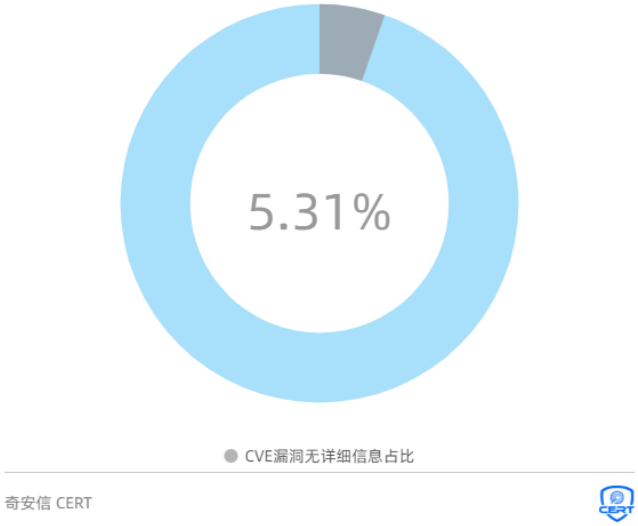

图 1-2 2021 年 CVE 漏洞无详细信息占比情况

2021 年奇安信 CERT 的漏洞库新增漏洞信息[1]21,664 条[2]（其中 20,206 条有效漏洞信息在 NOX 安全监测平台上显示），经 NOX 安全监测平台筛选后有 14,544 条敏感漏洞信息[3]触发人工研判，其中 2,124 条漏洞信息达到奇安信 CERT 的处置标准对其进行初步研判，并对初步研判后较为重要的 1,890 条漏洞信息进行深入研判。相较于 2020 年，初步研判的漏洞环比增长 159.02%，深入研判的漏洞环比增长 154.71%。2021 年奇安信 CERT 漏洞处置情况如图 1-3 所示：

1 奇安信 CERT 将互联网上包含漏洞相关内容的信息统称为漏洞信息
2 漏洞信息来源包含 NVD、CNVD、CNNVD 等开源漏洞库，以及各大互联网厂商和安全媒体披露的安全漏洞
3 敏感信息触发条件由漏洞影响的产品、漏洞热度、可能的影响范围等多个维度综合决定

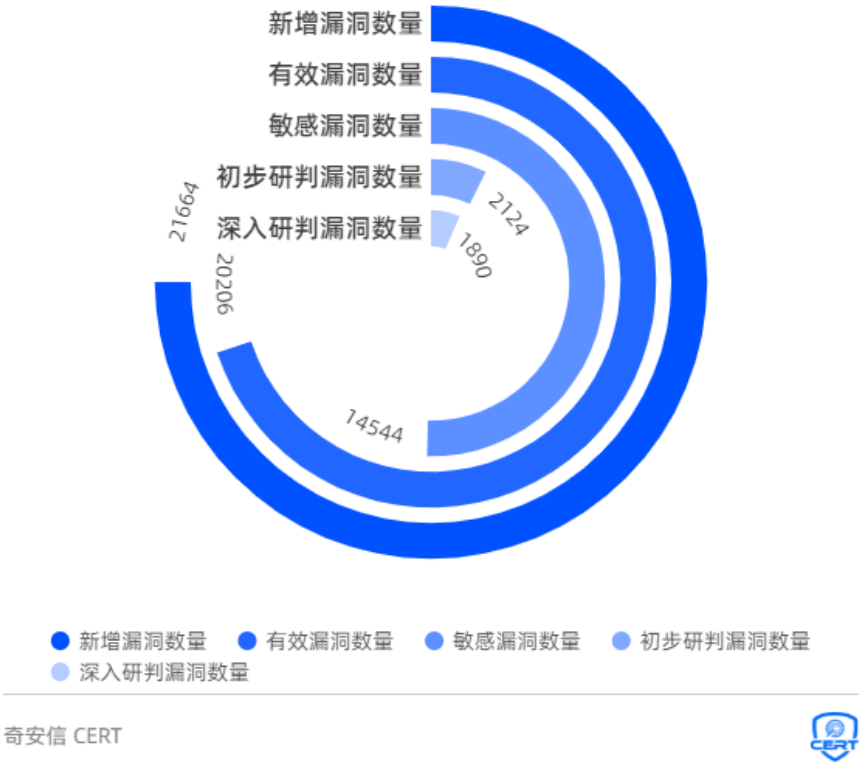

图 1-3 2021 年奇安信 CERT 漏洞处置情况

1.2 漏洞风险等级占比情况

奇安信 CERT 结合 CVSS 评价标准以及漏洞产生的实际影响将漏洞定级分为极危、高危、中危、低危四种等级，用来评价漏洞不同的影响程度。2021 年奇安信 CERT 研判过的 2,124 条漏洞信息中，各个等级占比情况如图 1-4 所示。

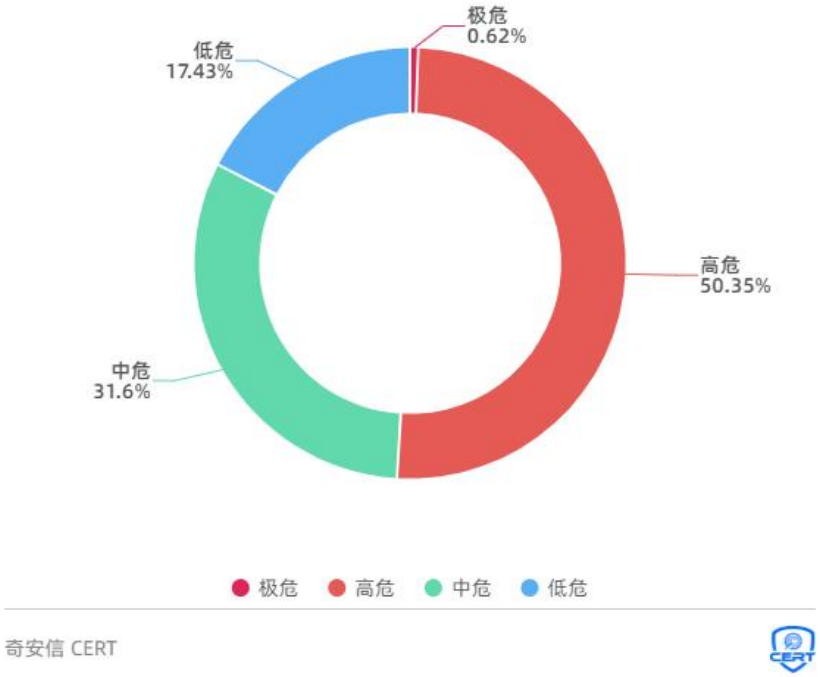

图 1-4 漏洞风险等级占比

其中，低危漏洞占比 17.43%，此类漏洞利用较为复杂或对可用性、机密性、完整性造成的影响较低；中危漏洞占比 31.60%，此类漏洞产生的影响介于高危漏洞与低危漏洞之间，可能需要一些复杂的配置或对漏洞成功利用的要求较高；高危漏洞占比 50.35%，此类漏洞极大可能造成较严重的影响或攻击成本较低；极危漏洞占比 0.62%，此类漏洞无需复杂的技术能力就可以利用，并且对机密性、完整性和可用性的影响极高。

1.3 漏洞威胁类型占比情况

将 2021 年度研判过的 2,124 条漏洞信息根据漏洞威胁类型进行分类总结，如图 1-5 所示，其中漏洞数量占比最高的五种类型分别为：代码执行、信息泄露、权限提升、拒绝服务、内存损坏。

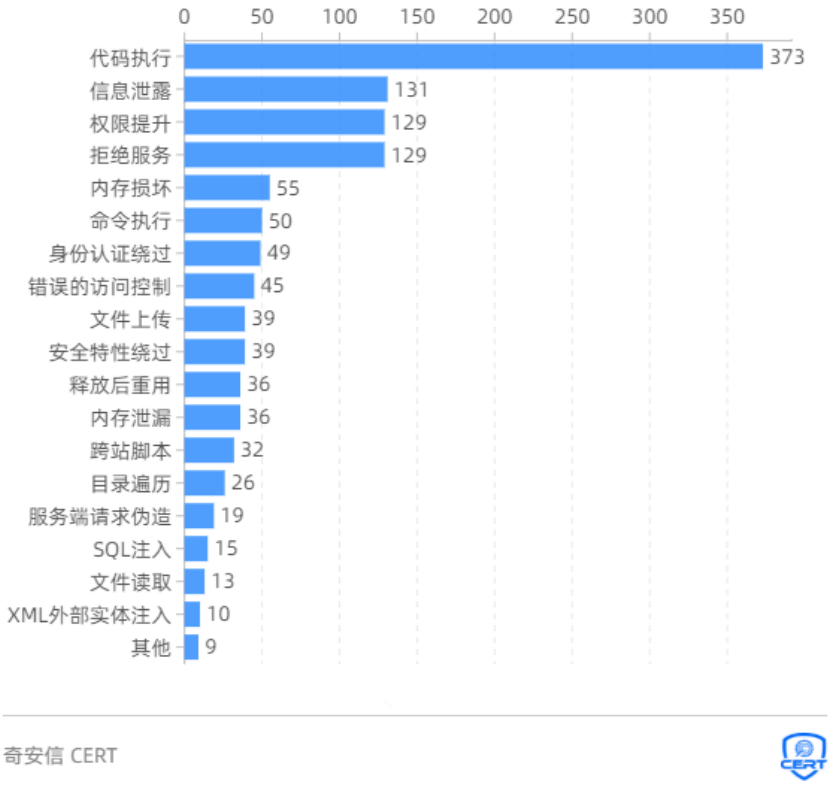

图 1-5 漏洞类型占比

漏洞数量排名靠前的威胁类型与 2021 Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses（2021 年 CWE 前 25 名最危险的软件漏洞）列表[4]具有较高相似性。这些类型的漏洞通常很容易被发现、利用，并且可以让攻击者完全接管系统、窃取数据或阻止应用程序运行，因而具有很高的危险性，是安全从业人员的重点关注对象。

1.4 漏洞影响厂商占比情况

将 2021 年度研判过的 2,124 条漏洞信息根据漏洞影响厂商进行分类总结，如图 1-6 所示，其中漏洞数量占比最高的前五家厂商为：Microsoft、Apache、Oracle、Apple、VMware。

4 http://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html

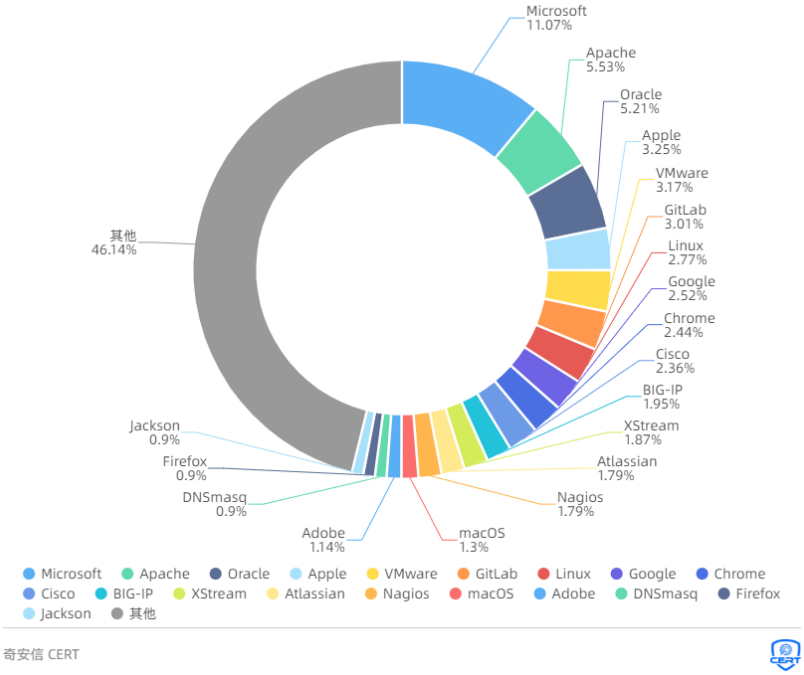

图 1-6 2021 漏洞影响厂商占比

Microsoft、Apache、Apple、Oracle 这类商业软件漏洞多发，且因为其有节奏的发布安全补丁，为漏洞处置的关注重点。开源软件和应用在企业中越来越多的使用，关注度逐渐攀升。部署在网络边界的网络设备在攻防行动中占据了重要地位，以获得了安全研究员更为重点的关注。

1.5 关键漏洞占比情况

2021 年奇安信 CERT 漏洞库新增的 21,664 个漏洞中存在 Exploit 漏洞数量为 4,779 个（占漏洞总量的 22.06%）、有在野利用漏洞数量为 337 个、0day 漏洞数量为 23 个、APT 相关漏洞数量为 88 个（见附录 2：2021 年度 APT 活动相关漏洞列表）。奇安信 CERT 将存在公开 Exploit/PoC、有在野利用、0day 漏洞、APT 相关，且漏洞相关软件影响面较大的漏洞定义为关键漏洞，2021 年共标记此类关键漏洞 5,227 个。

其中，部分 0day 漏洞在 NVD 上没有相应的 CVE 编号，未被国外漏洞库收录，为 2021 年攻防实战演练期间发现和使用的国产软件漏洞。此类漏洞具有较高威胁，如果被国家级的对手利用将导致非常严重的后果。

此外，有在野利用的 337 个漏洞中有 182 个漏洞有公开 Exploit，如图 1-7，还有近一半的在野利用漏洞并没有公开的 Exploit，处于私有状态，仅被某些 APT 组织或者个人使用。

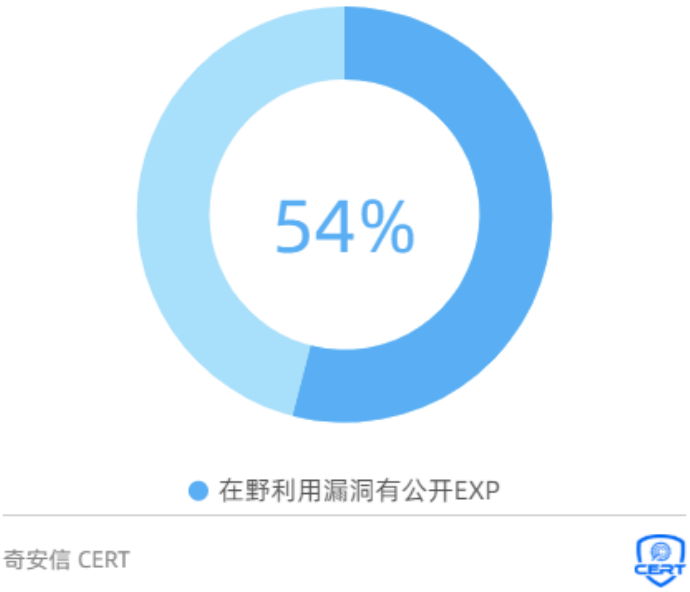

图 1-7 在野利用漏洞 Exploit 状态

关键漏洞的威胁度分布如图 1-8 所示，可以看出 Exploit 涉及到的漏洞威胁程度都集中在中高级别，分布较为平均，但真正被实际使用的漏洞，高威胁级别的占到百分之八十以上。从侧面印证了，漏洞修补应该将高威胁级别的漏洞放到高优先级的原则。

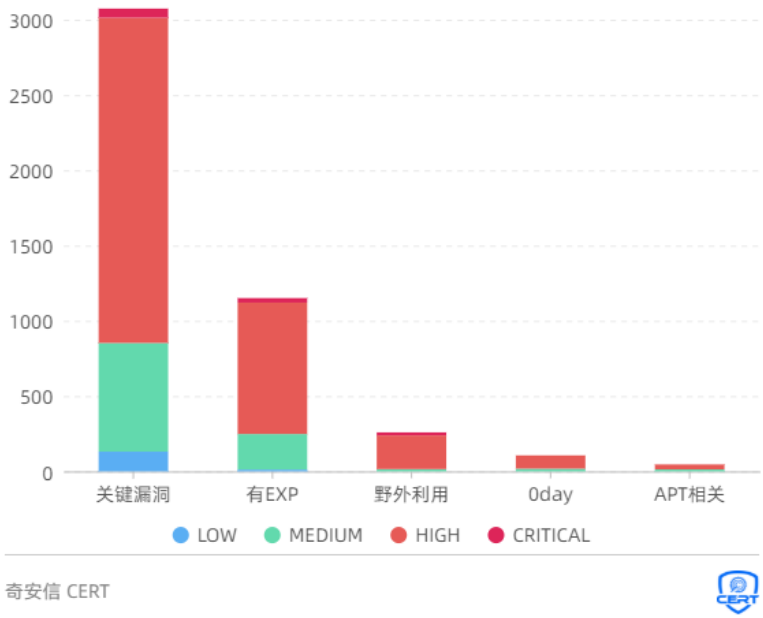

图 1-8 关键漏洞的威胁度分布

1.6 年度安全大事件

1.6.1 背景介绍

Apache Log4j 是 Apache 的一个开源 Java 日志记录工具，Apache log4j2 是 Log4j 的升级版本，日志记录主要用来担当集成开发环境中的调试器的作用，向文件或控制台打印代码的调试信息，Log4j 因其卓越的性能，使用极其广泛。

自 2021 年 12 月 9 日，Apache Log4j 远程代码执行漏洞（CVE-2021-44228）在互联网小范围内被公开后，其影响面迅速扩大，不到半个月的时间内，Apache Log4j 又陆续被曝出 4 个漏洞，如下表所示：

漏洞编号	威胁类型	CVSS 评分	是否默认配置受影响	漏洞威胁状态			
				技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-44228	代码执行	10.0	是	已公开	已公开	已公开	已发现
CVE-2021-45046	代码执行	9.0	否	已公开	已公开	未知	已发现
CVE-2021-4104	代码执行	8.1	否	已公开	已公开	未知	已发现
CVE-2021-45105	拒绝服务	7.5	否	已公开	已公开	未知	已发现
CVE-2021-44832	代码执行	6.6	否	已公开	已公开	未知	未知

国外给 Apache Log4j 远程代码执行漏洞（CVE-2021-44228）起了个颇能反

映其威胁的名字“Log4Shell”，奇安信 CERT 将其命名为“Poisoned Log”（毒日志）漏洞。此漏洞毫无争议地成为 2021 年热度最大的漏洞，也是近几年来最严重的网络安全威胁之一，因为如下多方面的考量使然：

1、无利用门槛的远程代码执行

与 HeartBleed 的信息泄露类漏洞不同，Log4j2 漏洞可以使攻击者在服务器上执行命令，导致系统机密性、可用性、完整性的完全破坏。而且，漏洞的利用门槛极低，默认配置下无需用户验证也没有其他限制条件。

2、利用稳定的设计错误类漏洞

log4j 漏洞不是不能稳定利用的内存破坏类漏洞，而是设计错误类漏洞，因此利用起来绝对稳定，只要漏洞存在就能稳定触发，就像为攻击者预留的后门。

3、log4j 是大量基础产品中的基础组件

根据奇安信代码安全实验室对开源组件库的分析显示：直接使用 log4j-core 的受影响版本开源组件接近 70000 个，形成指数级扩张的影响面，影响服务器级别至少千万级。

4、多源的不可控触发途径

log4j 的功能是记录各种日志信息，需要处理各种来源不可控的用户输入数据，导致输入的恶意数据通过最常见的 Web 服务端口进入，并可能层层穿透组件最终触发漏洞。

5、伴随 Java 的跨平台特性

Java 语言的特性之一就是跨平台，意味着相关的漏洞会同时影响 Windows 和 Linux 类平台。

1.6.2 事件描述

2021 年 12 月 9 日晚间，奇安信 CERT 监测到 Apache Log4j 远程代码执行漏洞（CVE-2021-44228），Apache Struts2、Apache Solr、Apache Druid、Apache Flink 等众多组件与大型应用均受影响。奇安信 CERT 于 12 月 9 日深夜复现确认漏洞后立即将技术信息上报相关主管部门。根据奇安信监测数据显示，截至 12 月 10 日中午 12 点，已发现近 1 万次利用该漏洞的攻击行为，应急响应中心已接到数十起重要单位的漏洞应急响应需求。补天漏洞响应平台负责人介绍，12 月 9 日深夜，仅一小时内就收到白帽黑客提交的百余条该漏洞的信息。漏洞时间线如图 1-9 所示：

图 1-9 Apache Log4j 漏洞发展时间线

研究人员发现，截至 2021 年 12 月 16 日，来自 Maven Central 的 35863 个可用软件包依赖于存在漏洞的 Log4j2 代码。这意味着 Maven Central 上超过 8%的软件包至少有一个版本受漏洞影响（此数字不包括所有 Java 软件包，例如直接分发的二进制文件）。就生态系统影响而言，8%是相当巨大的数字，因为对 Maven Central 生态的平均影响数值为 2%，中位数则低于 0.1%。因此，对于整个生态需要耗费多少时间来完成漏洞修复，目前也很难评估，在接下来相当长的一段时间内将陆续确认受影响的各类应用软件和系统。

据漏洞管理公司 Tenable 分析，所有评估的资产中大约有 10%受 Log4Shell 漏洞影响，包括各种服务器、Web 应用程序、容器和 IoT 设备，遍及大部分行业和地区。工业网络安全公司 Dragos 分析的数据发现，Log4j 漏洞会影响专有和开源软件，将使多个行业面临攻击风险，包括电力、水、食品和饮料、制造业和运输业。同时也影响了全球范围内关键信息基础设施，可能导致个人信息和重要数据泄露、金融紊乱、电网崩溃、交通瘫痪、通信中断。

1.6.3 事件影响

此漏洞对整个互联网带来极大安全威胁，直接动摇了以 Java 技术栈为重要组成部分的网络应用安全基础，堪比 2017 年核弹级漏洞“永恒之蓝”，大量的恶意代码已经将其纳入攻击传播的手段之一。

微软已监测到来自多个国家的黑客组织利用此漏洞进行攻击，如威胁组织

Phosphorus（又名 Charming Kitten、APT 35）。漏洞爆发初期，美国网络安全和基础设施安全局(CISA)命令所有联邦民事机构“必须在圣诞节前修补好受 Log4j 漏洞影响的相关系统”。新加坡网络安全局(CSA)也与关键信息基础设施(CII)部门针对 Log4j 漏洞举行紧急会议，并发布漏洞的警示公告。比利时国防部曾遭到严重的网络攻击，导致内部系统瘫痪。Bitdefender 的一份报告显示，Log4Shell 漏洞已经被用于 Khonsari 勒索软件攻击，预计未来 Windows 和 Linux 服务器上的勒索软件攻击将激增。某安全研究员发现一种正在开发中的自我传播蠕虫，来自 Salt Security 的 Yaniv Balmas 等研究人员表示 Log4j 蠕虫的出现并不是最坏的情况，因为此漏洞的攻击门槛极低，可访问互联网的任何人都可在几分钟内对数百万在线服务发起攻击，这跟蠕虫造成的影响极其相似——分布式且不可预测的，由于蠕虫以自动化全量扫描的方式工作，此漏洞的破坏程度甚至可能比蠕虫还要高。

十年前，一场地震和随后的海啸引发了福岛核电站的熔毁，至今仍在困扰该地区。同样，Log4Shell 漏洞的爆发对于网络安全行业简直就是“福岛时刻”，随着时间的推移，将演变出更复杂的攻击形式和影响范围。Log4Shell 漏洞事件揭示了企业级产品依赖开源代码库的高风险性。随着数字化转型和软件开发敏捷性的需求每年呈指数级增长，世界各地的企业在开发过程中不得不依赖开源库以快速迭代。如果把 2017 年 5 月 12 日的“永恒之蓝”漏洞所导致的“WannaCry”勒索蠕虫事件比作一次互联网核爆攻击，那么，由于 Log4j 在基础设施和应用程序中的大量使用，2021 年 12 月 9 日由 Log4Shell 漏洞引发的一大波网络攻击则可以比作是一次脏弹攻击，不仅在攻击的当时造成严重杀伤，还会在未来相当长的时间（以十年计）持续地对我们的网络安全形成威胁。现在是时候制定一套标准对基础架构中的每个开源组件进行清晰的评估整理，确保在开发生命周期的每一步都保证安全性。开源软件安全治理是一项任重道远的工作，需要国家、行业、用户、软件厂商都重视起来才能达到良好效果。

2. 2021年度关键漏洞回顾

2.1 重点关注厂商

2.1.1 微软漏洞回顾

微软（Microsoft）作为全球最大的电脑软件提供商、世界 PC（Personal Computer，个人计算机）软件开发的先导，其最为著名和畅销的产品为 Windows 操作系统和 Office 系列软件。截至 2021 年 7 月，全球桌面操作系统市场中，Windows 市场占有率为 74.79%，远高于其他操作系统。2021 年度，微软共发布了 800 多个漏洞的安全通告及补丁程序。虽然微软发布安全更新的时间是每月的第二个周二，但当出现紧急情况时（如发现影响较大的 0day 漏洞 EXP 被公开或出现在野攻击等），微软会发布紧急通告，如今年的 ProxyLogon、PrintNightmare、PetitPotam 等漏洞。根据漏洞的危害程度及影响力，奇安信 CERT 整理了微软本年度关键漏洞列表，如下所示：

产品	漏洞编号	威胁类型	攻击向量		
			攻击途径	身份认证	用户交互
Microsoft Exchange Server	CVE-2021-26855	身份认证绕过	网络	无需	无需
	CVE-2021-27065	任意文件写入	网络	低	无需
	CVE-2021-26857	代码执行	网络	低	无需
	CVE-2021-26858	任意文件写入	网络	低	无需
	CVE-2021-28480	身份认证绕过	网络	无需	无需
	CVE-2021-28481	身份认证绕过	网络	无需	无需
	CVE-2021-28482	代码执行	网络	低	无需
	CVE-2021-28483	代码执行	网络	低	无需
	CVE-2021-34473	身份认证绕过	网络	无需	无需
	CVE-2021-34523	权限提升	本地	低	无需
	CVE-2021-31207	任意文件写入	网络	高	无需
	CVE-2021-33766	信息泄露	网络	无需	无需
	CVE-2021-42321	代码执行	网络	低	无需
Active Directory Domain Services	CVE-2021-42287	权限提升	网络	低	无需
	CVE-2021-42278	权限提升	网络	低	无需
Microsoft SharePoint	CVE-2021-31181	代码执行	网络	低	无需
	CVE-2021-28474	代码执行	网络	低	无需

Server					
Windows Print Spooler	CVE-2021-1675	代码执行	网络	低	无需
	CVE-2021-34527	代码执行	网络	低	无需
	CVE-2021-34481	代码执行	网络	低	无需
	CVE-2021-36936	代码执行	网络	低	无需
	CVE-2021-36958	代码执行	网络	低	无需
Windows DNS Server	CVE-2021-24078	代码执行	网络	无需	无需
	CVE-2021-26877	代码执行	网络	无需	无需
	CVE-2021-26897	代码执行	网络	无需	无需
HTTP 协议栈	CVE-2021-31166	代码执行	网络	无需	无需
Internet Explorer	CVE-2021-26411	代码执行	网络	无需	需要
	CVE-2021-27085	代码执行	网络	无需	需要
Windows MSHTML platform	CVE-2021-33742	代码执行	网络	无需	需要
	CVE-2021-40444	代码执行	网络	无需	需要
Microsoft Office	CVE-2021-27059	代码执行	网络	无需	需要
Microsoft Excel	CVE-2021-42292	安全特性绕过	网络	无需	需要
Windows AppX Installer	CVE-2021-43890	欺骗	网络	无需	需要
Microsoft Defender	CVE-2021-1647	代码执行	网络	无需	需要
Windows Win32k	CVE-2021-1732	权限提升	本地	低	无需
	CVE-2021-28310	权限提升	本地	低	无需
	CVE-2021-40449	权限提升	本地	低	无需
Microsoft DWM Core Library	CVE-2021-33739	权限提升	本地	低	无需
Windows Kernel	CVE-2021-31955	信息泄露	本地	低	无需
	CVE-2021-33771	权限提升	本地	低	无需
	CVE-2021-31979	权限提升	本地	低	无需
Windows NTFS	CVE-2021-31956	权限提升	本地	低	无需
Microsoft Enhanced Cryptographic Provider	CVE-2021-31199	权限提升	本地	低	无需
	CVE-2021-31201	权限提升	本地	低	无需
Windows	CVE-2021-36934	权限提升	本地	低	无需
Windows Installer	CVE-2021-43883	权限提升	本地	低	无需
Windows Update Medic Service	CVE-2021-36948	权限提升	本地	低	无需
Windows Mobile Device Management	CVE-2021-43880	权限提升	本地	低	无需

根据产品特征以及攻击向量等因素可以将漏洞归为服务端漏洞、客户端漏洞

和提权类漏洞三类。依据上表中的标记，很容易区分这三类漏洞：

1. 服务端漏洞：一般允许远程攻击者通过网络发起攻击，并且漏洞利用不需要用户交互。在这种条件下，无需身份认证的漏洞是值得重点关注的，因为这种漏洞的利用条件相当宽松，只需要向受漏洞影响的服务端发送特制请求就可以触发漏洞，如果能稳定利用的话，这种漏洞将会是网络上的大杀器。
2. 客户端漏洞：一般需要攻击者诱导用户打开特制文件（用户交互）才能利用，对于一些加入了沙箱机制的关键客户端程序，如 IE、Office 等，攻击者还需配合权限提升漏洞来绕过沙箱并获得系统权限。
3. 提权类漏洞：一般认为攻击者在利用这类漏洞发起攻击前需要进行身份认证，但不需要用户交互，攻击者可利用这类漏洞将当前用户权限提升至更高级别的权限。

➢ **服务端漏洞**

我们重点关注企业中常用的产品或者在全球范围内部署量极大的服务端，如 AD 域服务、Microsoft Exchange Server、Microsoft SharePoint Server、Microsoft DNS Server 等等。Microsoft Exchange Server 和 Windows Print Spooler 是本年度安全研究人员以及黑客的重点关注对象，Microsoft Exchange Server 的几个未授权远程代码执行漏洞利用链已发现被多个黑客组织利用；PrintNightmare 漏洞自被披露以来热度一直都很高，随着更多的安全研究人员加入研究，Windows Print Spooler 系列漏洞层出不穷。

在这里，我们更倾向于关注无需身份认证且默认配置可触发的漏洞，由于此类漏洞利用门槛低，一旦稳定的漏洞利用程序被开发出来，甚至被公开在互联网，很容易被黑客利用起来发起大规模无差别攻击。

■ Microsoft Exchange Server

Microsoft Exchange Server 在全球拥有大量用户，是企业和学术机构最常用的电子邮件服务器。其运行在 Windows Server 上，使用 Active Directory 来存储和共享目录信息。作为最常用的电子邮件解决方案，Exchange Server 一直

都是黑客的首要目标。如果黑客发起攻击，可能导致用户敏感数据泄露，给企业和用户带来重大损失。

从 Exchange 历史漏洞来看，这些漏洞在利用上通常是需要授权的，这意味着黑客在攻击 Exchange 前需要获得身份认证信息。但由于新的攻击面出现，本年度 Exchange 接连被曝出 ProxyLogon、ProxyShell 等重大漏洞利用链，未经身份认证的远程攻击者可利用这些攻击链在易受攻击的 Exchange 服务器上执行任意代码。攻击者只需要能访问到目标设备的 443 端口即可发起攻击，不需要其他任何条件。更糟糕的是，APT 组织还利用这些漏洞发起大规模攻击，用于窃取电子邮件信息、窃取 Active Directory 数据库的副本、添加域账户、进一步横向移动等。

下表为本年度 Microsoft Exchange Server 的关键漏洞情况：

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-26855	身份认证绕过	9.1	已公开	已公开	已公开	已发现
CVE-2021-27065	任意文件写入	7.8	已公开	已公开	已公开	已发现
CVE-2021-26857	远程代码执行	7.8	已公开	已公开	已公开	已发现
CVE-2021-26858	任意文件写入	7.8	已公开	已公开	已公开	已发现
CVE-2021-28480	身份认证绕过	9.8	已公开	未知	未知	已发现
CVE-2021-28481	身份认证绕过	9.8	未公开	未知	未知	未知
CVE-2021-28482	远程代码执行	8.8	已公开	已公开	已公开	未知
CVE-2021-28483	远程代码执行	9.0	未公开	未知	未知	未知
CVE-2021-34473	身份认证绕过	9.1	已公开	已公开	已公开	已发现
CVE-2021-34523	权限提升	9.0	已公开	已公开	已公开	已发现
CVE-2021-31207	任意文件写入	6.6	已公开	已公开	已公开	已发现
CVE-2021-33766	信息泄露	7.3	已公开	已公开	已公开	未知
CVE-2021-42321	远程代码执行	8.8	已公开	已公开	已公开	已发现

- ProxyLogon

CVE-2021-26855 服务端请求伪造（SSRF）漏洞又称为“ProxyLogon”，攻击者可以利用这个漏洞绕过 Exchange Server 的身份验证获得管理员权限。配合 CVE-2021-27065 或 CVE-2021-26858 任意文件写入漏洞，未经身份认证的攻击者可将文件写入服务器的任意路径从而执行任意代码；配合 CVE-2021-26857 反序列化漏洞，未经身份认证的攻击者可通过发送恶意请求在 Exchange 服务器上以

SYSTEM 权限执行任意代码。

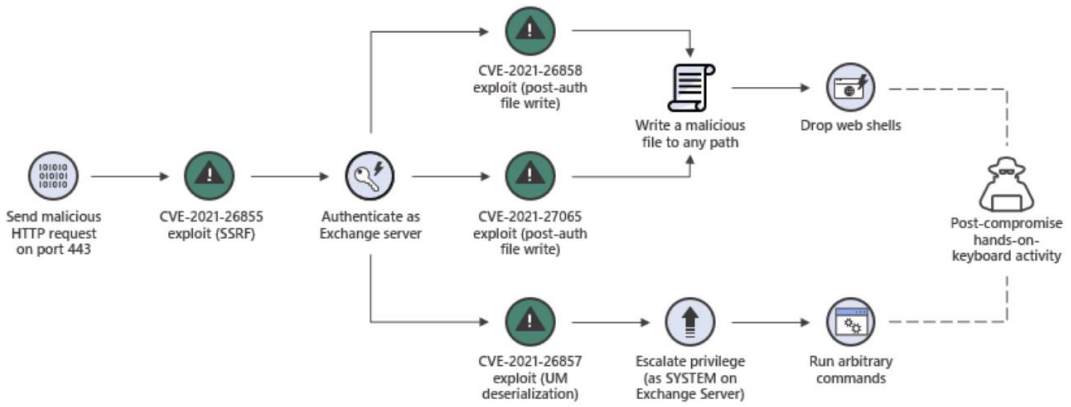

图 2-1 ProxyLogon 漏洞利用链

据 Volexity 安全研究人员披露，ProxyLogon 的相关攻击可追溯到 2021 年 1 月份[5]，且相关漏洞攻击持续进行。迫于这些漏洞影响巨大，微软于补丁日前一周（2021 年 3 月 3 日）公开了这些漏洞并发布告警。

- ProxyShell

与 ProxyLogon 类似，ProxyShell 是一个完整的 Exchange 漏洞利用链，包括 CVE-2021-34473 Microsoft Exchange ACL 绕过漏洞、CVE-2021-34523 Microsoft Exchange 权限提升漏洞以及 CVE-2021-31207 Microsoft Exchange 授权任意文件写入漏洞。这些漏洞细节以及 PoC 已公开，并且已经被用于野外攻击，BlackByte、LockFile 等勒索软件也被发现利用这些漏洞进行传播。通过组合这些漏洞，未经身份验证的远程攻击者可接管目标服务器，企业应高度重视这些漏洞。

- ProxyToken

“ProxyToken”是存在于 Exchange 中的一个信息泄露漏洞（CVE-2021-33766），微软官方已于 2021 年 7 月 13 日发布了此漏洞通告以及补丁程序。未经身份验证的攻击者可以对属于任意用户的邮箱执行配置操作。攻击者可利用此漏洞复制发送到目标邮箱账户的所有电子邮件，并将它们转发到由攻击者控制的账

5 https://unit42.paloaltonetworks.com/microsoft-exchange-server-attack-timeline/

户。

在默认配置下，攻击者需要控制一个与受害者相同的 Exchange 服务器的账户，然后利用此漏洞读取受害者收到的所有邮件。但如果管理员为 Exchange 配置了允许转发任意 Internet 目标的规则，攻击者不需要获取账号也可以读取受害者收到的所有邮件。

尽管暂时没有监测到利用此漏洞的攻击，但相关细节及 PoC/EXP 已经公开，奇安信 CERT 已验证其有效性。此漏洞存在较大被利用的风险，一旦被攻击者成功利用，企业将遭受重大损失。

- CVE-2021-42321

最后一个备受关注的漏洞是 CVE-2021-42321 Microsoft Exchange Server 远程代码执行漏洞，安全研究人员曾在 2021 年演示成功利用此漏洞攻破 Exchange 服务器，微软在 11 月发布通告时指出此漏洞已检测到漏洞利用。经过身份验证的远程攻击者，可利用此漏洞在目标服务器上执行任意代码。虽然利用此漏洞需要身份认证，但攻击者可以组合其他未授权漏洞发起攻击，企业还应及时修复这类漏洞。

■ Active Directory Domain Services

Active Directory 域服务（AD DS）是 Active Directory 中的核心组件，它存储和管理连接到网络的用户、设备和服务信息，使用户能够对网络上的资源进行身份验证和访问。Active Directory 是攻击者进行渗透、横向移动和数据泄露的一个关键目标。

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-42287	权限提升	7.5	已公开	已公开	已公开	未知
CVE-2021-42278	权限提升	7.5	已公开	已公开	已公开	未知

Active Directory 域服务权限提升漏洞（CVE-2021-42278、CVE-2021-42287）允许攻击者使用 AD 用户属性 sAMAccountName 欺骗来模拟域控制器，攻击者可通过组合利用这两个漏洞绕过安全限制提升至域管理员权限。此漏洞于 2021 年 11 月微软补丁日公开，12 月 12 日，国外安全研究员披露了这两个漏洞的细节以及

PoC/EXP，奇安信 CERT 已验证此 PoC/EXP 有效，漏洞存在较大被利用风险。成功利用此漏洞的攻击者可以以 SYSTEM 权限在域控机器上执行任意代码，危害极大。

■ Microsoft SharePoint Server

Microsoft SharePoint Server 是由微软提供的用以提供基本的门户网站和企业内网功能的软件。超过 200,000 个组织和 1.9 亿人将 SharePoint 用于 Intranet、团队网站和内容管理。

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-31181	代码执行	8.8	已公开	已公开	已公开	未知
CVE-2021-28474	代码执行	8.8	已公开	已公开	已公开	未知

作为内网中常用的服务端，Microsoft SharePoint Server 的安全也是不容忽视的。不过，Microsoft SharePoint Server 漏洞几乎都需要身份认证，经过身份认证的远程攻击者可通过创建 SharePoint 站点并发送特制的请求来利用这些漏洞，成功利用漏洞可在目标系统上执行任意代码。但由于 CVE-2021-31181 和 CVE-2021-28474 这两个漏洞的细节及 PoC 已经公开，且奇安信 CERT 已验证其有效性，尽管暂时没有监测到在野利用，考虑到漏洞的危害程度，用户还是应保持警惕。

■ Windows Print Spooler

Windows Print Spooler 是打印后台处理服务，管理所有本地和网络打印队列及控制所有打印工作。Spooler 服务(Spoolsv.exe)以 SYSTEM 权限运行，并且可通过网络进行访问，这允许攻击者远程发起攻击，攻击者利用这类漏洞可在目标机器上以 SYSTEM 权限执行任意代码。尽管漏洞利用需要授权，但具有攻击经验的黑客可采用多种方式获得身份认证信息。

PrintNightmare 是本年度 Spooler 中备受瞩目的一个远程代码执行漏洞。由于 Windows Print Spooler 服务对特权文件的操作不恰当，经过身份认证的攻击者可通过调用 RpcAddPrinterDriverEx 函数使 Spooler 服务加载恶意 DLL，从而在目标系统上以 SYSTEM 权限执行任意代码，2021 年 7 月 2 日，微软官方发布通告声称已经检测到了该漏洞的在野利用。此后，Windows Print Spooler 相继

被曝出很多漏洞。

以下为本年度 Windows Print Spooler 的关键漏洞情况：

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-1675	代码执行	8.8	已公开	已公开	已公开	已发现
CVE-2021-34527	代码执行	8.8	已公开	已公开	已公开	已发现
CVE-2021-34481	代码执行	8.8	已公开	已公开	已公开	未知
CVE-2021-36936	代码执行	8.8	已公开	未知	未知	未知
CVE-2021-36958	代码执行	8.8	已公开	已公开	已公开	已发现

CVE-2021-1675 是 Spooler 中 2021 年第一个受到广泛关注的远程代码执行漏洞，于 6 月份补丁日公开。起初，微软将其研判为权限提升漏洞。6 月 28 日，奇安信威胁情报中心红雨滴团队通过技术手段开发出此漏洞远程利用 EXP，并在 Twitter 上发布相关演示视频。6 月 29 日，国内安全研究员在网络上公开此漏洞远程利用 EXP，并将漏洞命名为 PrintNightmare。随后，微软将 CVE-2021-1675 更正为 Windows Print Spooler 远程代码执行漏洞。不过，7 月 2 日，微软发布了 Windows Print Spooler 服务远程代码执行漏洞（CVE-2021-34527）通告，将 PrintNightmare 指向 CVE-2021-34527，表示此漏洞与 CVE-2021-1675 攻击向量不同。尽管如此，安全研究人员依然认为 PrintNightmare 漏洞是由于微软由于没有完整修复 CVE-2021-1675 导致的。

此后，微软陆续发布 CVE-2021-34481 权限提升漏洞（随后也被更改为远程代码执行漏洞）和 CVE-2021-36958 远程代码执行漏洞（疑似为 CVE-2021-34481 的补丁绕过）通告。Microsoft Windows 允许缺乏管理权限的用户安装打印机驱动程序，虽然 Windows 强制驱动程序本身由受信任的来源签名，但 Windows 打印机驱动程序可以指定与设备特定队列关联的文件。这些文件可与强制执行数字签名的打印机驱动程序文件一起复制，不需要任何签名。此外，这些文件可用于覆盖在打印机驱动程序安装期间放置在系统上的任何签名验证文件。通过连接到恶意打印机，攻击者可在易受攻击的系统上以 SYSTEM 权限执行任意代码。

■ Microsoft DNS Server

Windows DNS Server 是微软提供的可运行在 Windows Server 上的 DNS 服务

器，它可以提供多种类型的 DNS 服务，包括缓存、动态 DNS 更新、区域传输和 DNS 通知。在 Active Directory 域中通常需要搭建 Windows DNS Server，当用户执行身份验证、更新或搜索时，计算机会使用 DNS 服务器来定位 Active Directory 域控制器。由于 DNS 服务的设计特性，漏洞利用通常不需要用户交互、不需要身份认证，并且 DNS 服务运行在 SYSTEM 权限下，攻击者在攻破 DNS 服务器后将会获得目标机器的 SYSTEM 权限。

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-24078	代码执行	9.8	未知	未知	未知	未知
CVE-2021-26877	代码执行	9.8	已公开	已公开	未知	未知
CVE-2021-26897	代码执行	9.8	已公开	已公开	未知	未知

与蠕虫级漏洞 SigRed 相同，CVE-2021-24078 Windows DNS Server 远程代码执行漏洞[6]也是 DNS 服务器在解析通过转发查询到的响应时存在的漏洞。攻击者仅需向目标 DNS 服务器发送特制数据包，即可利用该漏洞在目标系统上以系统账户权限执行任意代码，且漏洞利用无需交互、无需身份认证且在 Windows DNS 默认配置下可触发。安全研究人员已开发出 SigRed 漏洞利用程序，经奇安信 CERT 验证，此 EXP 可在实验环境下获得目标系统的 SYSTEM SHELL。在未来，黑客可能开发出更加稳定的漏洞利用程序。因而，用户还需警惕这一类漏洞。

CVE-2021-26877 和 CVE-2021-26897 等远程代码执行漏洞是 Windows DNS Server 在处理动态 DNS 更新时产生的，这两个漏洞的细节及 PoC 在漏洞发布时已公开。尽管微软官方给出的 CVSSv3 评分为 9.8 分，经奇安信 CERT 验证，启用安全动态更新可暂时缓解此漏洞（DNS 默认推荐配置），在这种场景下，攻击者在发起攻击前需经过身份认证。微软并不建议用户为 DNS 服务器配置不安全的动态更新，因而这类漏洞的触发前置条件较为严苛。

■ HTTP 协议栈

HTTP 协议栈常见于应用之间或设备之间通信，以及 Internet Information Services (IIS)中。在 2021 年 5 月份的微软补丁日中出现了一枚影响广泛的高危漏洞（CVE-2021-31166），此漏洞无需身份交互以及用户交互，且被微软官方

6 该漏洞由奇安信代码安全实验室研究员罗权发现并提交

标记为 Wormable 和 Exploitation More Likely，这意味着漏洞处利用可能性很大且有可能被恶意攻击者制作成可自我复制的蠕虫病毒进行大规模攻击。漏洞存在于 HTTP 协议栈驱动程序(http.sys)中，未授权的攻击者可构造带有 Accept-Encoding 的恶意请求包来攻击目标服务器。

此漏洞影响 2020 年以后发布的并且启用了 IIS 服务器的 Windows 或 Windows Server 主机。尽管利用此漏洞进行远程代码执行难度较大，但公开的 PoC 可稳定触发 BSoD，由于此漏洞不需要身份认证和交互，且可远程发起并稳定触发，还是值得关注的。

- **客户端漏洞**

在这一部分，我们关注的依然是企业员工常用的客户端软件，如 IE、Office。客户端类的漏洞一般都需要用户交互，攻击者通常会使用鱼叉式钓鱼攻击来利用这类漏洞，通过诱导用户打开特制文件或链接从而触发漏洞执行恶意代码，钓鱼攻击是网络安全的主要威胁之一。

比较特别的是，今年 1 月份微软公开了 ZINC 在针对安全研究人员的网络攻击中使用了 CVE-2021-26411 Internet Explorer 内存损坏漏洞。攻击者先是在 Twitter 的安全研究社区中建立声誉，然后再通过电子邮件、即时通讯工具以及博客等媒介发布恶意的 Visual Studio 项目以及利用浏览器漏洞的水坑网站，从而对目标用户发起攻击。这是黑客组织针对特殊目标群体的一次尝试，给防范意识较低的安全研究人员敲响了警钟。

以下为本年度 Windows 客户端相关的关键漏洞情况：

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-26411	代码执行	8.8	已公开	已公开	已公开	已发现
CVE-2021-27085	代码执行	8.8	未公开	未知	未知	已发现
CVE-2021-33742	代码执行	7.5	已公开	已公开	已公开	已发现
CVE-2021-40444	代码执行	8.8	已公开	已公开	已公开	已发现
CVE-2021-27059	代码执行	7.6	未公开	未知	未知	已发现
CVE-2021-42292	代码执行	7.8	已公开	未知	未知	已发现
CVE-2021-43890	安全特性绕过	7.1	已公开	未知	未知	已发现
CVE-2021-1647	代码执行	7.8	已公开	已公开	已公开	已发现

MSHTML（又称为 Trident）是微软旗下的 Internet Explorer 浏览器引擎，虽然 MHTML 主要用于已被弃用的 Internet Explorer 浏览器，但该组件也用于 Word、Excel 或 PowerPoint 等 Office 应用程序，在文档中呈现 Web 托管的内容。2021 年 4 月，Google TAG 发现了一项针对亚美尼亚用户的攻击，攻击利用了一个 Internet Explorer 0day 漏洞，漏洞编号为 CVE-2021-33742。恶意 Office 文档会在 Internet Explorer 中加载 Web 内容。恶意文档会对设备进行指纹识别，然后将此 Internet Explorer 网站发送给用户。2021 年 9 月，微软紧急发布 Microsoft MSHTML 远程代码执行漏洞通告，漏洞编号为 CVE-2021-40444，同时奇安信红雨滴团队已捕获多个鱼叉邮件样本。攻击者通过制作带有恶意 ActiveX 控件的 Microsoft Office 文档并诱导用户打开此文档来利用此漏洞。成功利用此漏洞的远程攻击者可在目标系统上以该用户权限执行任意代码。

Microsoft Office 是微软开发的一套基于 Windows 操作系统的办公套件，是企业员工通常使用的办公软件，全球使用量上亿。由于使用量巨大且可稳定利用的漏洞较多，其相关组件早已成为黑客攻击的焦点。CVE-2021-42292 Microsoft Excel 安全功能绕过漏洞是由于 Excel 在处理文件时输入验证不当造成的，微软在 11 月份发布通告时声称已经检测到在野攻击。攻击者可诱导用户打开特制 Excel 来利用此漏洞，成功利用此漏洞可以绕过 Excel 的安全机制。

APPX 文件是通用的 Windows 应用程序包，用于在桌面和移动版的 Windows 系统上分发和安装应用程序。ms-appinstaller 是 Microsoft 为简化应用程序安装流程、提高效率、避免磁盘浪费而提出的一种安装应用程序的 Web 协议。CVE-2021-43890 Windows AppX 安装程序欺骗漏洞允许攻击将恶意软件包伪装成合法软件。攻击者可以滥用 CVE-2021-43890 来创建具有合法软件图标的虚假恶意软件包、将软件包标记为受信任应用程序的有效证书等，这可以增加目标用户的信任度。微软在发布漏洞通告时指出已发现在野攻击，恶意攻击者正利用此漏洞传播 Emotet、Trickbot、Bazaloader 等恶意软件。微软最终选择禁用 ms-appinstaller 协议来避免这类漏洞。

Microsoft Defender Antivirus 是 Win10、Win11 以及 Windows Server 上的内置恶意软件扫描程序。作为 Windows 安全套件的一部分，它会扫描计算机上

可能造成威胁的文件或程序。Defender 的主动扫描为攻击者提供一个很好的攻击面，目标用户无需打开恶意文件，攻击者只需通过一些手段触发 Defender 的自动检测就可以进行漏洞利用，如 2021 年 1 月份公开的 CVE-2021-1647 Microsoft Defender 远程代码执行漏洞。攻击者可通过钓鱼攻击、邮件附件、IM 传输等方式进行利用，也可以用来光盘、U 盘的物理传播等。不过，Defender 在联网情况下会自动更新修复漏洞，理想情况下，微软如果能尽快发现并修补漏洞，那么漏洞的实际威胁就会大大降低。

- **提权类漏洞**

提权类漏洞允许用户将权限提升至更高级别，从而对原本系统中访问受限的资源进行访问或修改。攻击者在通过代码执行漏洞或其他手段获得目标系统上的较低权限之后可以利用此类漏洞提升权限进行下一步攻击。另一方面，由于 Internet Explorer、Microsoft Edge、Microsoft Office 和 Google Chrome 等软件已经引入沙箱机制，攻击者还需寻找权限提升漏洞来绕过沙箱的限制从而在目标系统上执行任意代码。

2021 年曝出很多在野权限提升漏洞，攻击者通常将这类漏洞和客户端漏洞组合使用，从而在目标系统上以 SYSTEM 权限执行代码。另外，奇安信 CERT 持续监测漏洞情报信息，相继发现并验证以下权限提升 0day 漏洞：

- Windows Installer 权限提升漏洞（CVE-2020-16902 的补丁绕过）
- CVE-2021-36934 Windows 权限提升漏洞（HiveNightmare）
- CVE-2021-43883 Windows Installer 权限提升漏洞（CVE-2021-41379 漏洞修复补丁的绕过），又称为 InstallerFileTakeOver
- CVE-2021-43880 Windows Mobile Device Management 权限提升漏洞

以下为本年度的关键提权类漏洞的情况：

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-1732	权限提升	7.8	已公开	已公开	已公开	已发现
CVE-2021-28310	权限提升	7.8	未公开	未知	未知	已发现
CVE-2021-33739	权限提升	8.4	已公开	已公开	已公开	已发现

CVE-2021-31955	信息泄露	5.5	未公开	未知	未知	已发现
CVE-2021-31956	权限提升	7.8	已公开	未知	未知	已发现
CVE-2021-31199	权限提升	5.2	未公开	未知	未知	已发现
CVE-2021-31201	权限提升	5.2	未公开	未知	未知	已发现
CVE-2021-33771	权限提升	7.8	未公开	未知	未知	已发现
CVE-2021-31979	权限提升	7.8	未公开	未知	未知	已发现
CVE-2021-36934	权限提升	7.8	已公开	已公开	已公开	未知
CVE-2021-36948	权限提升	7.8	未公开	未知	未知	已发现
CVE-2021-40449	权限提升	7.8	已公开	已公开	已公开	已发现
CVE-2021-43880	权限提升	5.5	已公开	已公开	已公开	未知
CVE-2021-43883	权限提升	7.8	已公开	已公开	已公开	已发现

Win32k 组件由 Windows NT 4.0 引入，用来管理窗口管理器（User）和图形设备接口（GDI）。由于设计原因，Win32k 驱动需要处理很多用户层的回调，这些回调给 Win32k 带来了很大的安全隐患。尽管在过去十几年中，已有大量安全研究员帮助微软修复了大量 Win32k 漏洞，本年度 Win32k 依然被曝出很多权限提升漏洞，如存在于 win32kfull.sys 中的 CVE-2021-1732 和 CVE-2021-40449。

CVE-2021-28310 也是存在于 Win32k 中的权限提升漏洞，由于缺乏边界检查，攻击者可通过调用 DirectComposition API 以受控偏移量写入受控数据来利用此漏洞。DirectComposition 组件由 Windows 8 开始引入，用于支持具有转换、效果和动画的高性能位图合成，DirectComposition API 由 win32kbase.sys 驱动程序实现。

2021 年早些时候，CVE-2021-1732 Windows Win32k 权限提升漏洞[7]和 CVE-2021-28310 Windows Win32k 权限提升漏洞[8]已发现被蔓灵花（BITTER）组织用来针对国内科研机构、政府部门，这两个漏洞分别由 DBAPPSecurity 威胁情报中心和卡巴斯基检测到并上报微软。攻击者可能将它们与其他浏览器进行组合利用以逃避沙箱或者获取系统特权。后来，卡巴斯基又发现了被 MysterySnail 利用的 CVE-2021-40449 Windows Win32k 权限提升漏洞[9]。

Microsoft Enhanced Cryptographic Provider（又称为 Enhanced Provider）

7 https://ti.dbappsecurity.com.cn/blog/articles/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack-cn/
8 https://securelist.com/zero-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/
9 https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

是微软制定的一种加密服务提供程序（CSP），用于实现数据的加密、解密、数字签名、验证和数据摘要等密码操作。Enhanced Provider 通过更长的密钥和额外的算法支持更强的安全性。

2021 年 6 月，微软公开了 Microsoft Enhanced Cryptographic Provider 权限提升漏洞（CVE-2021-31199、CVE-2021-31201）。这两个漏洞允许本地用户绕过 Microsoft Enhanced Cryptographic Provider 实施的安全限制并读取或修改其他受限制的信息。黑客组织将这两个漏洞与 CVE-2021-28550 Adobe Reader 任意代码执行漏洞组合使用，通过诱导用户打开特制的 PDF 文件（通常附在网络钓鱼电子邮件中）从而在目标系统上执行任意代码。

CVE-2021-31955 Windows 内核信息泄露漏洞（允许攻击者从系统中泄露信息）和 CVE-2021-31956 Windows NTFS 权限提升漏洞（ntfs.sys 中基于堆的缓冲区溢出漏洞，允许经过身份认证的攻击者进行提权）也于 2021 年 6 月公开。卡巴斯基研究人员检测到 PuzzleMaker Group 利用这两个漏洞进行攻击[10]，该组织将这两个漏洞与 Google Chrome V8 JavaScript 引擎远程代码执行漏洞组合利用，从而在受感染的 Windows 10 系统上执行具有 SYSTEM 权限的恶意软件模块，相关攻击最早可追溯到 4 月中旬。

2021 年 7 月，微软威胁情报中心(MSTIC)与微软安全响应中心(MSRC)公开了 SOURGUM 相关攻击。SOURGUM 组织通常向其客户销售能够侵入其目标的计算机、电话、网络基础设施和互联网连接设备的网络武器。此次攻击事件中，攻击者似乎使用了一系列浏览器和 Windows 漏洞在受害者机器上安装恶意软件，通过向目标用户发送 URL 消息（例如 WhatsApp）来触发浏览器漏洞，然后通过两个 0day 漏洞（Windows NT 操作系统 (NTOS)权限提升漏洞，CVE-2021-31979 和 CVE-2021-33771）逃脱浏览器沙箱并获得内核代码执行权[11]。

回顾 2021 年，微软修复了 800 多个漏洞，尽管今年修补的漏洞数量少于 2020 年，但其中一些漏洞导致了更加广泛的利用（如：ProxyLogon 漏洞），值得重点

10 https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/
11 https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

关注。微软整体的漏洞趋势，在一定程度上也反映出了安全团队未来一年应该注意的方向。通过对本年度微软关键漏洞的研究和利用情况进行总结，我们可以得出以下结论和观点：

1. **相比于客户端漏洞，服务端漏洞危害更严重**，因为整个漏洞利用的过程不需要用户参与。并且在 Windows 中，重要的服务端通常以 SYSTEM 权限运行，攻击者利用这种漏洞直接获得目标机器的 SYSTEM 权限。
2. 逻辑漏洞比内存破坏类漏洞在利用起来更加稳定。纵观 2021 年度的服务端漏洞，公开的且能稳定利用的漏洞几乎都是逻辑类漏洞。由此我们推测，**逻辑类漏洞方向上的研究仍将会是未来的一大趋势**。
3. 当产品出现超高关注度的重大漏洞时，会引来大量研究人员关注，研究人员对该漏洞的研究和分析过程中极有可能导致该产品的其它相关漏洞被发现。因此，**出现重大漏洞的产品极易在未来一段时间会出现更多漏洞**，如 Microsoft Exchange Server 在曝出 ProxyLogon 漏洞之后又出现了 ProxyShell 等漏洞，并且在未来，Microsoft Exchange Server 还将继续成为研究人员的重点研究对象。
4. **黑客会更加青睐利用门槛低且可以稳定利用的漏洞，并且在漏洞的细节及 PoC/EXP 公开之后，相关的漏洞攻击将呈现上升趋势**。
5. **网络钓鱼依然会是黑客盛行的攻击手段。**黑客组织依旧会使用目标用户感兴趣的主题精准打击，甚至会利用其他漏洞来增加攻击的迷惑性，使目标在毫无防备的情况下中招。企业还需培训员工提高自身的安全防范意识。
6. **黑客使用 0day 漏洞进行攻击的频率会增多**，这样即使系统已经更新到最新版本但依旧会受到攻击。反过来，当目标用户的安全意识提升，能及时为系统打上补丁，攻击者也只能选择使用 0day 武器。0day 漏洞的入侵检测还需要用户和安全厂商的共同努力。

2.1.2 Apache 漏洞回顾

Apache Software Foundation（ASF）是专门为支持开源软件项目而办的一

个非营利性组织，在 Apache 软件基金会主导下，已有 350 多个顶级开源项目毕业，包括全球最著名的网络服务器软件 Apache HTTP Server，可以说，Apache 软件基金会已然成为现代开源软件系统的基石。国际咨询公司 Gartner 研究数据显示，当前 99%的商业软件含有开源组件，75%则直接由开源代码组成，开源模式正成为软件产业发展的主要模式之一。

开源软件使用的广泛性，给了大量攻击者以可乘之机，当开源组件存在安全漏洞，组件之间又存在相互依赖关系，导致漏洞在组件之间存在传播风险。迄今为止“影响力最大的漏洞” Log4Shell 便是 Apache 软件基金会主导的开源日志组件 Log4j 中发现的漏洞，90%以上基于 Java 开发的应用平台都会受到影响。除此之外，ASF 管理的大量顶级开源项目如 Tomcat、Dubbo、Solr、Hadoop 等均被发现高危漏洞，安全隐患不可忽视。

漏洞编号	威胁类型	CVSS 评分	产品	漏洞威胁状态			
				技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-25646	代码执行	8.8	Apache Druid	已公开	已公开	已公开	已发现
CVE-2021-26919	代码执行	8.8		已公开	已公开	未公开	已发现
CVE-2021-36749	任意文件读取	6.5		已公开	已公开	未公开	已发现
CVE-2021-25641	代码执行	8.8	Apache Dubbo	已公开	已公开	已公开	未知
CVE-2021-30179	代码执行	8.8		已公开	已公开	已公开	未知
CVE-2021-30180	代码执行	6.8		已公开	已公开	未知	未知
CVE-2021-30181	代码执行	6.8		已公开	已公开	未知	未知
CVE-2021-36162	代码执行	8.8		已公开	已公开	已公开	未知
CVE-2021-36163	代码执行	6.8		已公开	已公开	已公开	未知
CVE-2021-26295	代码执行	9.8	Apache OFBiz	已公开	已公开	已公开	未知
CVE-2021-29200	代码执行	9.8		已公开	已公开	已公开	未知
CVE-2021-30128	代码执行	9.8		已公开	已公开	已公开	未知
CVE-2021-37608	任意文件上传	9.8		未公开	未知	未知	未知
CVE-2021-27905	服务端请求伪造	9.8	Apache Solr	已公开	已公开	已公开	已发现

- Druid

Apache Druid 是一个实时分析型数据库，旨在对大型数据集进行快速的查询分析("OLAP"查询)，最常被当做数据库来用以支持实时摄取、高性能查询和高稳定运行的应用场景。网络空间搜索引擎探测暴露公网资产 5w+，2021 年度曝出的漏洞大部分为中高危，威胁类型有任意文件读取、代码执行等。

由于 Apache Druid 默认情况下缺乏授权认证,对用户输入没有做严格限制，产生多个漏洞。攻击者可以发送特制请求，利用 Druid 服务器上进程的特权执行任意代码，即 Apache Druid 远程代码执行漏洞（CVE-2021-25646），此漏洞细节及 EXP 已在互联网公开。除此之外，攻击者可通过将文件 URL 传递给 HTTP InputSource 来绕过应用程序级别的限制，在未授权情况下利用该漏洞读取任意文件，最终导致服务器敏感信息泄露，即 Apache Druid 任意文件读取漏洞（CVE-2021-36749）。由于 Apache Druid 用户量很大，被活跃的黑客团伙攻击概率也相对较大。

- Dubbo

Apache Dubbo 是一款应用广泛的 Java RPC 分布式服务框架，其提供了面向接口代理的高性能 RPC 调用、智能容错和负载均衡、服务自动注册和发现、高度可扩展能力、运行期流量调度及可视化的服务治理与运维六大核心能力，可实现微服务治理的诸多诉求。目前 Dubbo 2.7 官方版本中支持多种 RPC 序列化协议，如：Hessian2、Fastjson、Kryo、FST、JDK、Protostuff/Protobuf、Avro、Gson，提供高灵活性的同时也伴随着很大的安全性风险。

2021 年 5 月 31 日,Dubbo 官方发布安全通告披露 Dubbo 中存在的多个漏洞，并在 2.7.10 及 2.6.10 版本中修复。2021 年 6 月 4 日，CVE-2021-25641 反序列化漏洞细节及 PoC 在互联网上公开，攻击者可在 Dubbo 协议中替换 Serialization 标识使用 Kryo 或 FST 等不安全的序列化方式来序列化数据，以此绕过 Hessian2 反序列化的限制，从而导致反序列化漏洞，执行任意代码。2021 年 6 月 22 日,漏洞发现者公开这些漏洞细节：如 CVE-2021-30179 Generic filter 处理泛型调用不当导致反序列化漏洞。

2021 年 8 月 30 日,国外安全研究人员披露 Dubbo 多个漏洞细节及 PoC：CVE-2021-36162 使用 SnakeYAML 加载 YAML 规则导致反序列化漏洞、CVE-2021-36163 使用 Hessian 协议的提供者程序中不安全的反序列化方式导致反序列化漏洞。

在 Dubbo 中 RPC 通信反序列化是最容易被攻击者利用的一个过程，用户在切换序列化协议或实现前，应充分调研目标序列化协议及其框架实现的安全性保障，并提前设置相应的安全措施。

- OFBiz

Apache OFBiz 是一个非常著名的电子商务平台，用于构建大中型企业级、跨平台、跨数据库、跨应用服务器的多层、分布式电子商务类 WEB 应用系统的框架。OFBiz 最主要的特点是 OFBiz 提供了一整套的开发基于 Java 的 web 应用程序的组件和工具。

2021 年 3 月 21 日，Apache OFBiz 官方发布 17.12.06 更新版本，修复了一处由 RMI 反序列化造成的远程代码执行漏洞。

2021 年 4 月 28 日，Apache OFBiz 官方披露两个由反序列化造成的远程代码执行漏洞。漏洞编号分别为：CVE-2021-29200、CVE-2021-30128，定级为高危。2021 年 4 月 29 日，漏洞发现者公开漏洞利用细节。这两个漏洞均是针对 CVE-2021-26295 补丁 Apache OFBiz 17.12.06 版本中对反序列化漏洞防护方法（添加 RMI 相关类的黑名单;增加白名单机制)的绕过。攻击者可通过构造恶意请求，触发服务端反序列化，从而执行任意代码。

- Solr

Solr 是一个高性能，采用 Java5 开发，基于 Lucene 的全文搜索服务器。同时对其进行了扩展，提供了比 Lucene 更为丰富的查询语言，同时实现了可配置、可扩展并对查询性能进行了优化，并且提供了一个完善的功能管理界面，是一款非常优秀的全文检索引擎。

2021 年 4 月 13 日，奇安信 CERT 监测到 Apache Solr 发布了安全更新通告，发布了多个漏洞，其中漏洞影响最严重的为 Apache Solr 服务器端请求伪造漏洞（CVE-2021-27905)，随后，该漏洞的 Poc 也公开在了互联网上，OFBiz 因为使用了 Solr 插件，也受该漏洞影响。

2021 年 5 月 8 日，奇安信 CERT 监测到 Apache Solr 全版本存在任意文件删除漏洞，Solr 默认安装后无需任何其它配置即可删除系统任意文件。在默认安装的情况下，未经身份验证的攻击者可以删除系统任意文件。

Solr 今年虽然未出现风险极大的命令执行漏洞，但是服务端请求伪造(SSRF)，任意文件删除的危害也是很大的，攻击者可以通过 SSRF 探测企业内网，

可以通过任意文件删除漏洞删除系统重要文件，对企业网络安全的影响也是非常高的。

2.1.3 Linux 漏洞回顾

作为开源生态系统的支柱之一，Linux 已成为当今世界主导云平台和服务器的最强大的操作系统之一。由于 Linux 具有免费开源、稳定、开放等优势，客户更倾向于将服务部署在 Linux 上。尤其是在云中，它可以为大多数基础设施提供动力。据 Trend Micro 统计，企业客户群的大部分为 Linux 用户，约为 61%，Windows 用户占 39%。Linux 已成为网络犯罪分子的一个非常有吸引力的目标。

2021 年，Linux 被曝出一系列漏洞，包括 eBPF、Netfilter、TIPC 等模块中的权限提升漏洞，这些漏洞细节及 EXP 都已公开，攻击者可利用这些漏洞成功提升至 ROOT 权限。除此之外，年初公开的 Sudo 本地权限提升漏洞（CVE-2021-3156）也吸引了广泛的关注度，研究人员们采用多种方式在多个系统上成功利用了此漏洞。

2021 年值得关注的 Linux 漏洞如下：

漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-3156	权限提升	7.8	已公开	已公开	已公开	未知
CVE-2021-31440	权限提升	7.0	已公开	已公开	已公开	未知
CVE-2021-3490	权限提升	7.8	已公开	已公开	已公开	未知
CVE-2021-34866	权限提升	7.8	已公开	已公开	已公开	未知
CVE-2021-22555	权限提升	7.8	已公开	已公开	已公开	未知
CVE-2021-33909	权限提升	7.8	已公开	已公开	已公开	未知
CVE-2021-3493	权限提升	7.8	已公开	已公开	已公开	未知
CVE-2021-26708	权限提升	7.0	已公开	已公开	未知	未知
CVE-2021-43267	远程代码执行	9.8	已公开	已公开	已公开	未知

- **sudo 本地权限提升漏洞（CVE-2021-3156）**

Sudo 的全称是"superuserdo"，它是 Linux 系统管理指令，允许用户在不需要切换环境的前提下以其它用户的权限运行应用程序或命令，通常是以 ROOT 用户身份运行命令。2021 年 1 月 26 日，Qualys 研究团队在互联网上公开 Sudo 堆

溢出漏洞(CVE-2021-3156，又称为”Baron Samedit”)的利用细节。经过身份验证的本地攻击者可以利用该漏洞实现本地权限提升，将本地普通用户权限提升到ROOT 权限。此漏洞由 2011 年 7 月发布的版本引入，影响过去十年的发布的所有 Sudo 版本。2 月 3 号，有国外有安全研究人员公开了该漏洞的 EXP，奇安信已验证该 EXP 有效。

- **Linux Kernel eBPF 本地权限提升漏洞**

eBPF 是一项革命性的技术，起源于 Linux 内核，可以在操作系统内核中运行沙箱程序。它用于安全有效地扩展内核的功能，而无需更改内核源代码或加载内核模块。今年有 3 个 eBPF 漏洞值得重点关注：

2021 年 5 月 27 号，ZDI 网站上公开了 CVE-2021-31440 的漏洞细节和 PoC，并在 Ubuntu20.10 上演示成功实现了 Kubernetes 容器逃逸。该漏洞是因为 eBPF 在 64 位边界转换为 32 位边界时存在错误。2021 年 6 月 9 号，该漏洞 ExP 在互联网公开，奇安信 CERT 已验证该 ExP 有效。

2021 年 7 月 20 日，国外安全研究员 chompie1337 在互联网上公开了 CVE-2021-3490 的漏洞细节和 EXP，该漏洞作者已在 Ubuntu20.04，Ubuntu20.10，Ubuntu21.04 默认配置上成功验证，并在 Ubuntu 21.04 上进行了演示。该漏洞是由于按位操作（AND，OR 和 XOR）的 eBPF ALU32 边界跟踪没有正确更新 32 位边界而导致，奇安信 CERT 已验证该 EXP 有效。

2021 年 12 月 8 日，flatt_security 公开了 CVE-2021-34866 的漏洞的利用细节。随后有安全人员公开了该漏洞的 ExP。值得注意的是，该漏洞已于 4 月份在 PWN2OWN 2021 上演示成功，且漏洞的细节和 Exp 已经公开。在默认配置下，经过身份验证的本地攻击者利用以上三个都能将普通权限权限提升到 root 权限。

- **Linux Kernel Netfilter 本地权限提升漏洞（CVE-2021-22555）**

2021 年 7 月 16 日，国外安全研究员 theflow 在互联网上公开该漏洞的利用细节和 ExP，该漏洞已存在近 15 年。Netfilter 是 Linux 2.4.x 引入的一个子系统，它作为一个通用的、抽象的框架，提供一整套的 hook 函数的管理机制，使得诸如数据包过滤、网络地址转换(NAT)和基于协议类型的连接跟踪成为了可能。

经过身份认证的本地攻击者可以利用该漏洞进行权限提升。值得注意的是，该漏洞已经在 kCTF 中被用于攻击 kubernetes pod 容器实现虚拟化逃逸，且该漏洞的细节和 ExP 已经公开，奇安信 CERT 已验证该 ExP 有效。

- **Linux Kernel Sequoia 本地权限提升漏洞（CVE-2021-33909）**

2021 年 7 月 20 日，Qualys 团队在互联网上公开了 Linux Kernel Sequoia 本地权限提升漏洞的技术细节，并在视频里面进行该漏洞利用的演示。该漏洞存在 Linux Kernel 内核文件系统层，经过身份验证的本地攻击者可以利用该漏洞实现本地权限提升，将本地普通用户权限提升到 root 权限。值得注意的是，该漏洞的细节和 ExP 已公开且多个 linux Kernel 版本受到影响。

- **Linux Kernel overlayfs 本地权限提升漏洞（CVE-2021-3493）**

2021 年 4 月 19 日，国外安全研究人员公开了 Linux Kernel overlayfs 本地权限提升漏洞的技术细节，随后两天网上就有安全研究人员公开了 ExP。该漏洞存在 Ubuntu 的 Overlayfs 文件系统，OverlayFS 是一个面向 Linux 的文件系统服务，实现一个面向其他文件系统的联合挂载。经过身份验证的本地攻击者可以利用该漏洞实现本地权限提升，将本地普通用户权限提升到 root 权限。值得注意的是，该漏洞的细节和 ExP 已公开且漏洞利用复杂度低。

- **Linux Kernel VSOCK 本地权限提升漏洞（CVE-2021-26708）**

2021 年 2 月 9 日，国外安全研究人员公开了 Linux Kernel VSOCK 本地权限提升漏洞的漏洞利用技术细节。VM 套接字允许虚拟机和管理程序之间的通信。虚拟机和主机上的用户级应用程序都可以使用 VM Sockets API，可促进之间的快速高效通信来宾虚拟机及其主机。该漏洞存在于 Linux Kernel VSOCK 中，经过身份验证的本地攻击者可以利用该漏洞实现本地权限提升，将本地普通用户权限提升到 root 权限。值得注意的是，该漏洞的利用技术细节和 PoC 已公开。

- **Linux Kernel TIPC 远程代码执行漏洞（CVE-2021-42367）**

2021 年 11 月 4 日，国外安全研究人员公开了 Linux Kernel TIPC 远程代码执行漏洞（CVE-2021-42367）的漏洞细节。TIPC 作为内核模块实现，存在于所有主要 Linux 发行版中。它可以配置为通过 UDP 或直接通过以太网传输消息。

消息传递是顺序保证、无丢失和流控制的。延迟时间比任何其他已知协议都短，而最大吞吐量可与 TCP 相媲美。主要应用在集群上。经过身份验证的本地攻击者可以利用该漏洞实现本地权限提升和远程代码执行。值得注意的是，该漏洞的利用技术细节和 ExP 已公开。奇安信已验证该 ExP 有效。

2.2 供应链安全

当今社会，网络安全威胁和风险日益突出，并向政治、经济、文化、社会、生态、国防等领域传导渗透，而这些领域都离不开关键信息基础设施，随着 2021 年 8 月 17 日《关键信息基础设施安全保护条例》的发布，关键信息基础设施所使用的产品和服务安全都建设离不开供应链安全，供应链安全治理，关乎国家安全和行业的发展，过去几年里，供应链攻击事件发生愈发频繁，让我们不得不将目光关注至供应链攻击。

供应链攻击，也称价值链攻击或第三方攻击，发生在有攻击者通过可访问企业系统和数据的外部合作伙伴或者供应商的信息，通过这种攻击方式，攻击者不仅能轻易获取到企业中的敏感数据，而且由于使用该供应商产品的厂商较多，攻击造成的影响面也比一般通用漏洞造成的影响高的多，一家供应商受到攻击，影响的是成百上千家使用了该供应商产品的厂商，在这一背景下，企业面临的网络威胁日益严重。

漏洞编号	威胁类型	CVSS 评分	厂商	漏洞威胁状态			
				技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-35211	代码执行	9.8	Solarwinds	已公开	已公开	未知	已发现
CVE-2021-35392	内存损坏	8.1	Realtek	已公开	已公开	已公开	已发现
CVE-2021-35393	内存损坏	8.1		已公开	已公开	已公开	已发现
CVE-2021-35394	命令执行	9.8		已公开	已公开	已公开	已发现
CVE-2021-35395	代码执行	9.8		已公开	已公开	已公开	已发现
CVE-2021-29505	代码执行	7.5	Xstream	已公开	已公开	已公开	已发现
CVE-2021-21347	代码执行	6.1		已公开	已公开	已公开	已发现
CVE-2021-39144	代码执行	8.5		已公开	已公开	已公开	已发现
CVE-2021-39149	代码执行	8.5		已公开	已公开	已公开	已发现

- Solarwinds

Solarwinds Serv-U 是目前众多的 FTP 服务器软件之一.通过使用 Serv-U,

用户能够将任何一台 PC 设置成一个 FTP 服务器，这样,用户或其他使用者就能够使用 FTP 协议,通过在同一网络上的任何一台 PC 与 FTP 服务器连接,进行文件或目录的复制,移动,创建,和删除等。

2021 年 7 月 9 日，奇安信 CERT 监测到 Solarwinds 发布了安全风险通告，其中修复了 Serv-U 产品中远程代码执行漏洞，漏洞编号为 CVE-2021-35211。未授权的攻击者可利用该漏洞在目标服务器上执行任意代码，该漏洞已监测到在野利用，且后续 Solarwinds 在安全通告处新增了样本 IOC。

漏洞时间线如图 2-2 所示：

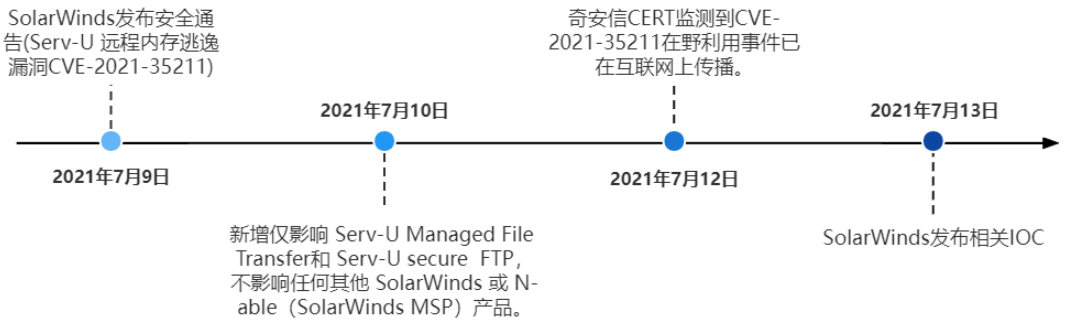

图 2-2 Solarwinds Serv-U 漏洞时间线

SolarWinds 是企业常用的组件，并且该产品的漏洞经常被用于供应链攻击，给企业带来的损失是非常巨大的，2020 年 12 月，黑客通过木马化的 SolarWinds Orion 软件入侵了公司网络，同时美国联邦调查局（FBI）、国家情报局局长办公室（ODNI）与美国国土安全部网络安全与基础设施安全局（CISA）联合发布声明，首次正式确认被黑客植入木马的 SolarWinds 造成多个美国联邦政府机构的网络遭受入侵，2021 年 3 月，SolarWinds 报告了去年供应链攻击的费用为 350 万美元，其中包括与补救和事件调查相关的费用，2021 年 7 月，遭受 CVE-2021-35211 攻击的企业已经超过了 18000 家,并且其中约 1/3 的企业并未使用 SolarWinds，可见供应链攻击的危害之大。

- **Realtek sdk**

2021 年 8 月 17 日，奇安信 CERT 监测到 iot-inspector 发布了关于 Realtek

SDK 多个漏洞的风险通告，该通告披露了 Realtek SDK 栈溢出漏洞(CVE-2021-35395)为主的一系列漏洞的细节。其中至少有 65 家厂商、数十万台设备受到影响，漏洞危害极大，并已发现在野利用。

漏洞时间线如图 2-3 所示：

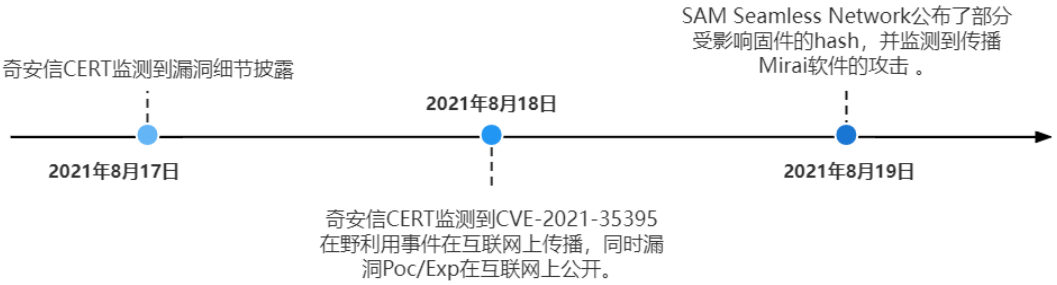

图 2-3 Realtek SDK 漏洞时间线

Realtek SDK 漏洞的攻击事件让我们不得不再次将目光放回到供应链安全，一旦上游的组件存在漏洞，那么危害是可以被无限放大的，本次 Realtek SDK 栈溢出漏洞(CVE-2021-35395)，该漏洞利用简单，无需交互即可获取到目标服务器权限，并可以在被厂商发现之前被攻击者迅速集成至攻击框架中，实施批量扫描，对于企业网络安全管理者来说，应该关注厂商发布的安全通告，及时检查企业内设备是否受影响，并联系设备厂商获取到升级补丁更新，非必要的设备不暴露在公网中。

- **Xstream**

XStream 是一种 OXMapping 技术，是 Java 类库，用来处理 XML 文件序列化的框架在将 javaBean 序列化，或将 XML 文件反序列化的时候，不需要其它辅助类和映射文件，使得 XML 序列化不再繁琐。由 CVE 数据可知 2021 全年共曝出 28 个漏洞，大部分为中高危，威胁类型有代码执行、命令执行以及 SSRF 等。

今年发布的系列漏洞主要为反序列化导致的代码执行，当用户使用 XStream 时默认未设置白名单安全框架，未授权的远程攻击者构造特定的 XML 数据发送至目标主机反序列化解析执行，PoC 在漏洞发布当天均在官网公开，未及时更新的用户受到大量攻击测试。Xstream 官方一度采用黑名单的方式来进行防护，间接

导致爆发大量黑名单绕过漏洞。不过自 XStream 1.4.18 开始默认开启白名单的安全框架，此后便不再有黑名单绕过，该产品漏洞热度逐渐减退。作为开源代码库成员之一，XStream 被企业系统和商业软件大量引用，其漏洞将间接影响无数开源或商用系统，影响力不可忽视。

2.3 中间件

现今为促进应用组件间的无缝集成，提升处理计算业务效率，开发集成相关技术不断发展，中间件成为这些新系统架构中必不可少的一环。中间件是连接不同的软件组件或应用程序的重要组件，位于操作系统之上的软件层，可形象称之为“软件胶水”，通常用于支持复杂的分布式业务软件应用程序。也正因如此，中间件安全问题不容小觑。

2021 年度，Oracle 融合中间件发布 191 个漏洞的安全更新补丁，这其中影响最为严重的是反序列化漏洞。漏洞利用通常无需身份验证，远程攻击者通过构造特定协议数据可导致命令执行甚至接管服务器。Apache HTTP Server 发布 17 个漏洞的安全通告，其中以 CVE-2021-41773 及其绕过 CVE-2021-42013 舆论热度最高。Apache Tomcat 发布 7 个漏洞的安全通告，以拒绝服务漏洞为主。2021 年值得关注的漏洞如下：

漏洞编号	威胁类型	产品	CVSS 评分	漏洞威胁状态			
				技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-2109	代码执行	Oracle WebLogic Server	7.2	已公开	已公开	已公开	未知
CVE-2020-14756	代码执行		9.8	已公开	已公开	已公开	未知
CVE-2021-2136	代码执行		9.8	未公开	未知	未知	未知
CVE-2021-2135	代码执行		9.8	已公开	已公开	已公开	未知
CVE-2021-2382	代码执行		9.8	未公开	未知	未知	未知
CVE-2021-2397	代码执行		9.8	未公开	未知	未知	未知
CVE-2021-2394	代码执行		9.8	已公开	已公开	已公开	未知
CVE-2021-35617	代码执行		9.8	未公开	未知	未知	未知
CVE-2021-41773	信息泄露	Apache HTTP Server	7.5	已公开	已公开	已公开	已发现
CVE-2021-42013	信息泄露		9.8	已公开	已公开	已公开	已发现
CVE-2021-40438	服务端请求伪造		9.0	已公开	已公开	已公开	已发现
CVE-2021-42340	拒绝服务	Apache Tomcat	7.5	已公开	已公开	已公开	已发现

- Weblogic

WebLogic 是美国 Oracle 公司出品的一个基于 JAVAEE 架构的中间件，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。其将 Java 的动态功能和 Java Enterprise 标准的安全性引入大型网络应用的开发、集成、部署和管理之中。WebLogic 是业界用于构建和部署企业级 Java EE 应用的理想应用服务器。

近年来，WebLogic 频繁被曝出高危漏洞，Oracle WebLogic 官方定期推出补丁供客户升级防护漏洞。这其中以反序列化漏洞影响最为严重。WebLogic 7001 端口默认接收 T3、IIOP、HTTP 等协议数据，WebLogic T3 协议及基于 CORBA 的 IIOP 协议是 WebLogic 实现 Java RMI 使用的主要通信协议，攻击者可通过构造特定协议数据与 WebLogic 服务器进行通信，这其中若未进行正确过滤则可能产生反序列化漏洞。

2021 年 1 月 18 日曝出 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 IIOPInputStream 进入反序列化逻辑前进行了转化。

可以发现这些漏洞的攻击利用复杂度都极低，攻击者构造特定数据即可执行任意代码。这期间 Oracle WebLogic 各组件的安全性不断提升，而安全研究人员对 WebLogic 的迭代更新也持续关注着，之后仍然可能出现新的利用姿势。

- Apache HTTP Server

Apache HTTP Server（HTTPd）是一种用于 Unix 和 Windows 的开源 Web 服务器，是使用最为广泛的 Web 服务器之一。

2021 年 10 月 4 日 Apache 官方发布 Apache HTTP Server 2.4.50 更新版本，披露 2.4.49 版本中存在路径遍历漏洞（CVE-2021-41773），同时表明该漏洞在未修复前已发现在野外利用。通过资产测绘工具发现互联网上至少存在 112,000 台服务器受该漏洞影响。该漏洞在 2.4.49 版本中引入，由于对路径规范化处理不当，在非默认配置情况下，攻击者可读取任意文件。公告发布后，该漏洞的概念验证代码在互联网上传播。

随后不久，10 月 7 日，Apache 官方发布另一个安全更新，推出 Apache HTTP Server 2.4.51 版本，修补 Apache HTTPd 2.4.50 版本中可能存在的远程代码执行漏洞。Apache 官方以 CVE-2021-42013 标识该漏洞，并将其命名为路径遍历及远程代码执行漏洞。该漏洞影响 Apache HTTP Server 2.4.49 和 2.4.50 版本，利用双编码形式绕过了 CVE-2021-41773 的补丁即 2.4.50 版本，同时表明若 Apache HTTPd 开启了 cgi 支持，未经身份认证的远程攻击者可构造恶意请求执行命令，控制服务器。此时漏洞细节、PoC 及 EXP 均已在互联网上传播，并已发现在野利用。

- Apache Tomcat

Tomcat 是 Apache 软件基金会 Jakarta 项目中的一个核心项目，作为目前比较流行的 Web 应用服务器，深受 Java 爱好者的喜爱，并得到了部分软件开发商的认可。网络空间搜索引擎探测暴露公网资产 177w+，2021 全年关于该产品热度较大的漏洞为 Apache Tomcat 拒绝服务漏洞（CVE-2021-42340）。2021 年 10 月，官方发布 Apache Tomcat 拒绝服务漏洞（CVE-2021-42340）安全通告，由于历史 bug 63362 的修复，一旦 WebSocket 连接关闭，用于收集 HTTP 升级连接的对象就不会针对 WebSocket 的连接释放，从而引发了内存泄漏，目前漏洞的 PoC 和 EXP 已经在互联网公开和传播，此漏洞会破坏 Tomcat 服务可用性，造成服务崩溃。Tomcat 从初版发布到现在已有二十多年历史，在世界范围内被广泛使用，大量框架及应用也在直接或间接的使用该产品，如 Spring Boot 则默认内置了 Tomcat 服务器。某公司测绘数据显示，在当前互联网中，至少有超过 100

万个 Tomcat 服务器正在运行使用，这也意味着漏洞波及范围远不止于此。

2.4 云原生及虚拟化

近几年，企业业务上云渐渐成为趋势，企业上云有很多优势，比如提高资源整合利用率、快速部署、高效维护、成本低等，往往用一个云管理平台就能管理所有机器，在便捷高效的同时也随之会面临一些新的安全问题。企业上云涉及到云原生技术和虚拟化技术，云原生的代表技术包括容器、服务网格（Service Mesh）、微服务（Microservice）、不可变基础设施和声明式 API。虚拟化依赖软件来模拟硬件功能并创建虚拟计算机系统，这使 IT 组织能够在单个服务器上运行多个虚拟系统以及多个操作系统和应用。企业上云主要面临三个主要安全问题：云管理平台安全，容器安全，虚拟机安全。攻击者可以通过虚拟机/容器攻击云管理平台，然后通过云管理平台控制所有机器。利用容器逃逸漏洞，从容器逃逸到直接宿主机，然后通过控制直接宿主机控制该宿主机下的所有容器。 利用虚拟机逃逸漏洞，从虚拟机逃逸到物理机，然后可以通过横向渗透到其他物理机。

2021 年出现许多云原生和虚拟化漏洞，今年值得关注的漏洞如下：

漏洞编号	威胁类型	影响产品	CVSS 评分	漏洞威胁状态			
				技术细节	PoC 状态	EXP 状态	在野利用
QVD-2021-35915	身份认证绕过	Hadoop Yarn	9.8	已公开	已公开	未知	已发现
CVE-2021-2310	权限提升	VirtualBox	7.5	已公开	未知	未知	未知
CVE-2021-2145	权限提升		7.5	已公开	未知	未知	未知
CVE-2021-2442	拒绝服务		6.0	已公开	未知	未知	未知
CVE-2021-28476	代码执行	Microsoft Hyper-V	9.9	已公开	已公开	未知	未知
CVE-2020-8562	权限提升	Kubernetes	2.2	已公开	已公开	未知	未知
CVE-2021-25735	权限提升		6.5	已公开	已公开	已公开	未知
CVE-2021-25737	信息泄露		4.8	未公开	未知	未知	未知
CVE-2021-25741	容器逃逸		9.9	已公开	未知	未知	未知
CVE-2021-20291	拒绝服务	CRI-O and Podman	6.5	已公开	未知	未知	未知
CVE-2021-30465	容器逃逸	runc	8.5	已公开	已公开	已公开	未知
CVE-2021-21287	SSRF	MinIO	7.7	已公开	已公开	已公开	未知
CVE-2021-38112	代码执行	AWS WorkSpaces	8.8	已公开	已公开	已公开	未知

CVE-2021-21972	代码执行	VMware	9.8	已公开	已公开	已公开	未知
CVE-2021-21973	SSRF		5.3	未公开	未知	未知	未知
CVE-2021-21974	代码执行		8.8	已公开	已公开	未知	未知
CVE-2021-21975	SSRF		8.6	已公开	已公开	已公开	已发现
CVE-2021-21985	代码执行		9.8	已公开	已公开	已公开	已发现
CVE-2021-21998	身份认证绕过		9.4	未公开	未知	未知	未知
CVE-2021-22048	权限提升		7.1	未公开	未知	未知	未知
CVE-2021-22005	代码执行		9.8	已公开	已公开	已公开	已发现
CVE-2021-22017	权限提升		7.3	已公开	已公开	已公开	未知
CVE-2021-21998	身份认证绕过		9.8	未公开	未知	未知	未知
CVE-2021-34824	信息泄露	Istio	8.8	未公开	未公开	未公开	未发现
QVD-2021-20125	代码执行	Yapi	8.7	已公开	已公开	已公开	已发现

- **Apache Hadoop Yarn RPC**

Apache Hadoop Yarn RPC 存在未授权访问漏洞，Apache Hadoop Yarn RPC 接口在默认情况下对外开放服务且不需要身份认证，未授权的攻击者可以编写 Yarn Client 并且向 Apache Hadoop Yarn RPC Serve 提交 Application，即可在目标 Hadoop 服务器上远程执行代码。由于 Apache Hadoop 通常用于集群，此漏洞若成功利用可能控制 Apache Hadoop Yarn 服务器。值得注意的是，该漏洞的技术细节和 PoC 已公开。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**

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。

- **Microsoft Hyper-V**

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，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。Hyper-V 是 Microsoft 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。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。值得注意的是，该漏洞的技术细节和 PoC 已公开，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。

- Kubernetes

Kubernetes，也称为 K8s，是一个开源系统，用于自动化部署、扩展和管理容器化应用程序，在集群上应用非常广泛。今年有 4 个 Kubernetes 漏洞和一个 Kubernetes 引擎库漏洞值得关注。2021 年 4 月，Kubernetes 社区披露 kube-apiserver 代理绕过漏洞（CVE-2020-8562），攻击者可以利用该漏洞访问 Kubernetes 托管集群服务的租户的 apiserver。2021 年 5 月，Kubernetes 社区披露 Kubernetes Admission Webhook 认证绕过漏洞（CVE-2021-25735）和 EndpointSlice 认证信息泄露漏洞（CVE-2021-25737），通过利用 Kubernetes Admission Webhook 认证绕过漏洞，攻击者可以绕过验证准入 Webhook 检查并允许对 Kubernetes 节点进行更新操作。通过利用 EndpointSlice 认证信息泄露漏洞，即使 Kubernetes 已经阻止在本地主机或本地链路范围内创建端点 IP，攻击者也可以重定向 pod 流量。这将允许攻击者劫持集群的网络流量，从而可能导致敏感数据泄漏，攻击者也能窃取凭证，利用该凭证在内网中横向移动。2021 年 9 月，Kubernetes 社区披露 Kubernetes 逃逸漏洞（CVE-2021-25741），攻击者可以创建一个带有子路径卷挂载的容器，以访问卷外的文件和目录，包括主机文件系统上的文件和目录。容器引擎 CRI-O and Podman 拒绝服务漏洞（CVE-2021-20291），攻击者可能会将恶意映像拉到多个不同的节点，使所有节点崩溃并破坏集群。

- runC 容器

2021 年 5 月 30 日，国外安全研究人员公开了 runC 容器逃逸漏洞的漏洞细节和 PoC，runC 是对于 OCI 标准的一个参考实现，是一个可以用于创建和运行容器的 CLI。docker 的底层是使用 runC 来管理镜像的创建，启动，监控及删除。

攻击者可以利用该漏洞实现容器逃逸，获取到 docker、k8s 主机的访问权限。

- MinIO

2021 一月 30，国内安全研究人员公开了 MinIO SSRF 漏洞的漏洞细节和 PoC，MinIO 提供高性能、S3 兼容的对象存储。MinIO 原生于 Kubernetes，是唯一可用于每个公共云、每个 Kubernetes 发行版、私有云和边缘的对象存储套件，在全球应用非常广泛。攻击者可以利用该漏洞在集群容器里执行任意命令。

- AWS WorkSpaces

AWS WorkSpaces 存在远程代码执行漏洞，Amazon WorkSpaces 部署在 Amazon Virtual Private Cloud (VPC) 内，本地设备上不存储任何用户数据。这有助于提高用户数据的安全性并减少您的整体风险表面积。如果受害者从浏览器打开攻击者定制的恶意 WorkSpaces URI，攻击者就能够在受害者的操作系统上执行代码。

- VMware

2021 年 2 月 23 日，VMware 官方发布安全通告披露 VMware vCenter Server 远程代码执行漏洞（CVE-2021-21972），未授权的攻击者可以通过开放 443 端口的 vCenter Server 服务器向其发送请求，从而在服务器上写入 WebShell，最终造成远程任意代码执行。通过资产测绘工具搜集到公网上易受影响的 VMware vCenter Server 服务器超过 6700 台。2 月 24 日，漏洞发现者在互联网上披露漏洞利用细节。当天，安全研究人员上传漏洞概念验证代码至 GitHub，与此同时 Bad Packets 发现了针对此漏洞的大规模扫描活动。

2021 年 5 月 25 日，VMware 官方发布安全公告，其中披露 CVE-2021-21985 VMware vCenter Server 远程代码执行漏洞的详细信息。未授权的攻击者可以通过开放的 443 端口在服务器上执行任意代码。截止 5 月 26 日，Rapid7 Labs 搜集到互联网上大约 6000 台 vCenter Server 服务器受影响。2021 年 6 月 2 日，安全研究人员公开 CVE-2021-21985 的概念验证代码。随后 6 月 3 日，Bad Packets 发现在野利用。

2021 年 9 月 21 日，VMware 官方发布安全通告修复 vCenter Server 中的 19

个漏洞，其中 CVE-2021-22005 影响最为严重。VMware vCenter Server 对上传文件的验证不足，具有 vCenter Server 443 端口的访问权限的攻击者可以向 vCenter Server 上传特制的恶意文件，执行任意代码。国外安全研究人员披露概念验证代码（PoC），这种方式需要开启客户体验改善计划（CEIP）功能。9 月 24 日，国外安全研究人员公开另一种导致远程代码执行的方式，并公开部分 PoC 以及演示视频。这种方式中无需任何配置，结合 CVE-2021-22017 rhttpproxy 绕过漏洞，攻击者访问 analytics 服务接口，将恶意代码通过日志记录的方式写入指定 JSP 文件中，从而导致远程代码执行。同时，VMware 官方表示已监测到在野利用。

- Istio

Istio 是一个开源服务网格，它可以控制微服务之间数据的共享方式。其附带的 API 可以将 Istio 集成到任何日志记录平台、遥测或策略系统中。 在设计上，Istio 可以在多种环境中运行：企业本地、云托管、Kubernetes 容器，或虚拟机上运行的服务等。

2021 年 6 月 24 日，奇安信 CERT 监测到监控到 Istio 官方发布安全更新通告，修复了 Istio 中的信息泄露漏洞，漏洞编号为 CVE-2021-34824，攻击者可利用授权客户端从 Gateways 或 DestinationRules 的 credentialName 配置中越权访问到私钥及 TLS 证书，从而导致信息泄漏。

虽然 Istio 中的信息泄露漏洞(CVE-2021-34824)是一个信息泄露漏洞，但是该漏洞泄露的是 TLS 证书及私钥，可能会导致加密传输中的数据被攻击者窃取并且解密为明文，甚至当 CA 机构发现证书泄露后，是有权利吊销该证书的。Istio 在云环境及企业内网中是很常用的组件，所以该组件的安全问题也是值得重视的。

- Yapi

Yapi 是一款使用起来非常方便的接口管理平台，很多大型企业也在使用该平台作为接口管理工具，2021 年 7 月 8 日，奇安信 CERT 监测到 YApi 接口管理平台存在远程命令执行 0day 漏洞，该漏洞利用时需要权限，但是默认配置下，攻击者可以通过注册接口获取权限。

需要注意的是，漏洞发布时处于 0day 状态，虽然有开发者在官方代码仓库提交了修复代码，但因为 Yapi 项目已经处于无人维护的状态，所以修复代码并未及时合并到主分支中。同时该漏洞也监测到了在野利用，很多企业因此遭受了网络攻击，由于 Yapi 的开发者长时间未维护该项目，所以有开发者自发了建立了 Yapi-pro（Yapi 的长期维护版本），奇安信 CERT 建议还在使用 Yapi 的开发者们及时更新到 Yapi 的 Pro 版本。

开源项目虽然使用方便，但是同时也是存在安全风险的，特别是长时间无人维护的项目，该类项目一旦爆发了漏洞，官方不能及时更新，受影响企业也不能第一时间修复，这给国内的互联网安全态势带来了极大的风险，所以在使用开源项目前，开发者应该评估该项目的安全性，并及时关注官方的安全通告。

2.5 网络设备及应用

2021 年是疫情发生的第二年，由于疫情，越来越多的企业和公司开始尝试远程和线上办公，对于在公司外进入生产环境或者公司内网的需求激增，很多黑客也瞄准了这一需求，加大了挖掘网络设备及应用相关漏洞的力度，在 2021 年相继披露了许多黑客利用相关漏洞进行在野利用事件，通过入侵边界网关设备，黑客可以获取进入企业内网的初始权限，由此可能造成更大的威胁。在 2022 年里，相信会有更多漏洞被黑客利用，木桶的盛水的上限由最短一块木板决定，企业网络安全性由最薄弱的一块决定，企业应该加大边界网关安全的投入，对于网络设备和应用进行加固，如今网络安全行业快速发展，各大公司相继建立了自己的“城墙”，同时黑客也在快速扩充自己的“军火库”，网络安全是相互对抗的，相信在 2022 年，终将邪不压正。

2021 年值得关注的网络设备及应用漏洞如下：

漏洞编号	威胁类型	产品	CVSS 评分	漏洞威胁状态			
				技术细节	PoC 状态	EXP 状态	在野利用
QVD-2021-7834	命令执行	JumpServer	高危	已公开	已公开	已公开	已发现
CVE-2021-22986	远程代码执行	F5 Networks	9.8	已公开	已发现	未知	已发现
CVE-2021-22987	命令执行		9.9	已公开	已发现	未知	未知
CVE-2021-22988	命令执行		8.8	未公开	未知	未知	未知
CVE-2021-22989	命令执行		9.1	未公开	未知	未知	未知

CVE-2021-22990	命令执行		7.2	未公开	未知	未知	未知
CVE-2021-22991	缓冲区溢出		9.8	未公开	未知	未知	未知
CVE-2021-22992	缓冲区溢出		9.8	已公开	未知	未知	未知
CVE-2021-22893	远程代码执行	Pulse Connect Secure SSL VPN	10	已公开	已发现	未知	已发现
QVD-2021-35927	文件上传	FatPipe MPVPN	8.8	未公开	未知	未知	已发现
CVE-2021-3064	远程代码执行	Palo Alto Networks GlobalProtect Portal VPN	9.8	未公开	未知	未知	未知

- JumpServer

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，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，如携程、小红书、顺丰等，将超大规模的资产迁移至新平台，可见用户量巨大。目前此漏洞的 PoC 和 EXP 已经在互联网公开和传播，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 Networks

F5 Networks 是全球领先的应用交付网络（ADN）领域的厂商，为全球大型企业、运营商、政府与消费品牌提供更加快速、安全以及智能的应用解决方案。在全球范围内，F5 Networks 公司的产品应用于金融业、政府机构等多个重要行业中，众多大型企业均有使用 F5 Networks 的解决方案，F5 Networks 的 BIG-IP/BIG-IQ 产品尤其畅销。由于 F5 Networks 公司产品的在企业网络中的特殊性，众多 APT 组织、勒索组织均喜爱研究该公司产品相关漏洞进行利用。

在 2021 年 3 月份，披露有 APT 组织利用 F5 BIG-IP 漏洞进行在野攻击事件，未经身份验证的攻击者可以通过 BIG-IP 管理界面或自身 IP 地址对 BIG-IP 的

iControl REST 接口进行访问，通过该漏洞在目标服务器上执行任意系统命令，创建或删除文件以及禁用服务，攻击者可以利用该漏洞获取入口权限，通过 BIG-IP 可以控制网络流量，在 APT 攻击事件曝光同月该漏洞的分析及 PoC 公开在互联网上。

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，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。和 CVE-2021-22987 利用方法类似的漏洞是 CVE-2021-22988，经过身份验证的攻击者可以使用控制界面利用 CVE-2021-22988，通过 BIG-IP 管理端口或自身 IP 访问 TMUI，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。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，通过 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。

当 BIG-IP 系统配备了 Advanced WAF 或 BIG-IP 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，利用 CVE-2021-22990 在目标服务器上通过执行任意系统命令，创建或删除文件，或禁用服务，在该条件下攻击者还可以利用 CVE-2021-22992，构造恶意的 HTTP 请求触发缓冲区溢出，从而造成拒绝服务，在某些情况下攻击者可以导致造成远程代码执行。在 BIG-IP 中，流量管理微内核（TMM）URI 规范化可能会错误地处理对虚拟服务器的请求，从而触发缓冲区溢出，导致 DoS 攻击这就是 CVE-2021-22991。在某些情况下，攻击者可能绕过基于 URL 的访问控制或实现远程代码执行。由于 BIG-IP 在企业内应用广泛， 且通过 BIG-IP/IQ 攻击者可以管理本地流量，当 BIG-IP 出现漏洞时对企业网路的威胁将是巨大的。

- **VPN 漏洞回顾**

虚拟专用网络(VPN)的功能是：在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。通过 VPN，可以安全加密自身流量数据、访问企业内网、安全数据传输等，由于 VPN 的特性，使得 APT 组织或者勒索组织喜欢利用

VPN 漏洞获取进入目标网络的入口权限。2021 年是疫情发生的第二年，越来越多企业增设远程办公职位，使得 VPN 应用范围越来越广，对于企业应用的 VPN，一旦出现 0day 影响范围将是巨大的，通过 VPN 漏洞可以顺利绕过企业的边界安全防护进入企业内网，所以 VPN 漏洞对企业的影响将会越来越大。

- **CVE-2021-22893 Pulse Connect Secure SSL VPN 身份认证绕过漏洞**

Pulse Connect Secure SSL VPN 是部署最广泛的 SSL VPN 之一，允许远程和移动用户通过身份验证随时随地使用任何基于 web 的设备安全访问公司资源。在 2021 年 4 月份监测到有 APT 组织利用 CVE-2021-22893 Pulse Connect Secure SSL VPN 身份认证绕过漏洞进行 APT 攻击，APT 组织利用该漏洞获取目标网络的初始访问权限。该漏洞利用无需用户交互，未授权利用该漏洞只需要发送特殊的 HTTP 请求即可，成功利用将在目标 Pulse Connect Secure 网关上执行任意代码，由于该设备在企业网络上的特殊性，利用该漏洞将对整个企业网络造成危害。

- **FatPipe MPVPN 文件上传漏洞**

FatPipe MPVPN 能够聚合两条或多条任意类型和任意组合的数据线，为 VPN 提供最高级别的安全性、冗余和速度，能提高 VPN 安全性，FatPipe MPVPN 在世界范围内的多个行业拥有大量客户。在 2021 年 11 月份，曝光 FatPipe VPN 存在文件上传漏洞，该漏洞允许具有只读权限的经过身份验证的攻击者上传任意文件到 FatPipe VPN 服务器，通过该漏洞攻击者可以获得具有 root 权限的 webshell。在 2021 年 11 月份，FBI 发表声明称，发现 APT 组织利用该漏洞进行攻击的事件，攻击时间至少可以追溯到 2021 年 5 月份，由于 VPN 在企业网络的特殊作用，成功利用该漏洞将对整个企业网络造成危害并且该漏洞有实际在野利用事件发生，该漏洞影响范围极大。

- **CVE-2021-3064 Palo Alto Networks GlobalProtect Portal VPN 远程代码执行漏洞**

Palo Alto Networks GlobalProtect Portal VPN 是业内极为出名的 VPN，在多家大型企业均有部署。在 2021 年 10 月份，来自 Randori 的 安全研究人员披露了该 VPN 的一个 0day 漏洞编号 CVE-2021-3064，攻击者可以通过组合 HTTP

请求走私来触发缓冲区溢出，从而利用此漏洞，通过利用此漏洞攻击者能够在目标服务器上以 root 权限执行任意代码。另外由于虚拟化设备缺乏地址空间随机化（Address Space Layout Randomization，ASLR），使得这个漏洞任意在虚拟化设备上利用，由于通过 VPN 攻击者可以进入企业网络内部，一旦 VPN 出现漏洞对于企业用户来说影响将是巨大的。

2.6 企业级应用及办公软件

在 2021 年度，企业中常用的应用及办公软件陆续曝出漏洞。由于疫情许多行业增设了线上渠道，web 端所占比重加大，浏览器作为 web 端入口显得尤其重要，一旦出现漏洞，将会影响数以亿计的 PC，所以许多 APT 组织喜欢利用水坑攻击组合 Chrome 浏览器漏洞攻击特定对象群体，以获取目标企业中的敏感信息。在 Chrome 的在野利用漏洞中，大部分漏洞只需要受害者使用 Chrome 打开恶意网站即可触发，组合沙箱逃逸或本地提权类漏洞，攻击者即可获得在目标电脑的执行权限，该类漏洞利用简单，危害极大。

OA 系列协同办公系统广泛应用于中小企业日常办公，网络空间搜索引擎探测暴露公网资产 10w+，由 CNVD 数据可知 2021 全年共曝出 65 个漏洞，大部分为中高危漏洞，一旦恶意利用，企业可能会受到较大的影响。Atlassian 产品在 2021 年虽然披露的漏洞不多，但高危漏洞热度居高不下。GitLab 官方披露 154 个漏洞，其中大部分漏洞需要低权限身份认证，但仍出现个别无需授权的远程代码执行漏洞，危害较大。Exim 在 2021 年度共披露了 22 个 CVE，在 Exim 的 22 个漏洞里面，部分无需身份验证即可利用，该类漏洞危害巨大，还有部分漏洞只能本地利用，故危害较小，所幸在 22 个 CVE 中有 21 个由安全研究员发现，没有被黑客提前挖掘到，对企业服务没有造成太大影响，只需升级 Exim 到安全版本即可。

2021 年企业级应用及办公软件值得关注的漏洞如下：

漏洞编号	威胁类型	产品	CVSS 评分	漏洞威胁状态			
				技术细节	PoC 状态	EXP 状态	在野利用
CVE-2021-21148	代码执行	Chrome	8.8	未公开	未知	未知	已发现
CVE-2021-21220	代码执行		8.8	已公开	已公开	已公开	已发现
CVE-2021-21224	代码执行		8.8	已公开	已公开	未知	已发现

CVE-2021-37975	代码执行		8.8	已公开	未知	未知	已发现
CVE-2021-37976	信息泄露		6.5	未公开	未知	未知	已发现
CVE-2021-30632	代码执行		8.8	已公开	已公开	未知	已发现
CVE-2021-30633	释放后重用		9.6	未公开	未知	未知	已发现
CVE-2021-26084	代码执行	Atlassian Confluence	9.8	已公开	已公开	已公开	已发现
CVE-2020-36239	代码执行	Atlassian Jira	9.8	未公开	未知	未知	未知
CVE-2021-26086	文件读取		5.3	未公开	已公开	未知	未知
CVE-2021-22205	代码执行	GitLab	10	已公开	已公开	已公开	已发现
CVE-2020-28007	本地权限提升	Exim	7.8	已公开	已发现	未知	未知
CVE-2020-28008	本地权限提升		7.8	已公开	已发现	未知	未知
CVE-2020-28018	代码执行		9.8	已公开	已发现	未知	未知
CVE-2020-28020	代码执行		9.8	已公开	已发现	未知	未知
CVE-2020-28024	命令执行		9.8	已公开	已发现	未知	未知

- **OA 系列协同办公系统**

在今年 CNVD 公开的漏洞中，大部分为中高危，威胁类型有文件上传、命令执行以及 SQL 注入等，其中针对文件上传威胁类型居多，其中 CNVD-2021-49104 热度较大。2021 年 11 月 26 日，奇安信 CERT 监测到此漏洞在野利用的事件在互联网上传播，由于系统未能正确处理上传模块中输入的数据，未授权的攻击者可以构造恶意数据包发送给服务器，实现任意文件上传，并且获得服务器的权限。次日，由于漏洞细节及 PoC 公开，并且利用难度低，导致漏洞影响面扩大。2021 年 06 月 01 日，奇安信 CERT 监测到 CNVD-2021-30167 细节公开，攻击者可通过访问特定 URL，实现远程命令执行。

2021 年值得关注的 OA 系列协同办公系统漏洞如下：

漏洞编号	威胁类型	漏洞评级	漏洞威胁状态			
			技术细节	PoC状态	EXP状态	在野利用
CNVD-2021-49104	文件上传	高危	已公开	公开	未知	已发现
CNVD-2021-32063	命令执行	高危	未公开	未公开	未知	未发现
CNVD-2021-01627	文件上传	高危	已公开	已公开	未公开	已发现
CNVD-2021-45266	命令执行	高危	已公开	已公开	未公开	已发现
CNVD-2021-51370	代码执行	高危	已公开	已公开	未公开	已发现
CNVD-2021-30167	代码执行	高危	已公开	已公开	未公开	已发现

- **Google Chrome**

Google Chrome 是一款由 Google 公司开发的网页浏览器，Google Chrome 的

特点是简洁、快速。Google Chrome 支持多标签浏览，每个标签页面都在独立的“沙箱”内运行，在提高安全性的同时，一个标签页面的崩溃也不会导致其他标签页面被关闭。此外，Google Chrome 基于更强大的 JavaScript V8 引擎，该引擎被众多浏览器所使用。根据 statcounter 的数据显示，截止至 2021 年 11 月 Google Chrome 在世界范围内浏览器市场占有率为 64.06%，为世界上使用率第一的浏览器，一旦出现漏洞，影响范围极大。由于浏览器在 web 中的特殊定位以及远超其他浏览器的市场占有率，众多 APT 组织尤其喜欢研究 Chrome 浏览器漏洞，配合其他漏洞组成利用链进行 APT 攻击。

在 2021 年度内，Chrome 被曝光出多起 APT 组织利用 Chrome 漏洞进行 APT 攻击事件，于 2021 年 2 月曝光的 CVE-2021-21148 Chrome 远程代码执行漏洞，该漏洞由国外安全研究员 Mattias Buelens 于 1 月 24 日向谷歌报告，微软在 1 月 28 日披露 APT 组织 ZINC 可能将该漏洞利用链托管在攻击者网站上来攻击漏洞研究人员，并且谷歌指出已经发现有攻击者尝试在野利用该漏洞，该漏洞源于 Chrome 的 V8 引擎中的堆溢出漏洞，攻击者可以构造恶意页面插入恶意 JavaScript 尝试在 V8 引擎中触发堆溢出，从而在受害者机器上远程执行代码，该漏洞不仅影响 Chrome 浏览器还影响所有基于 V8 引擎开发的软件，例 Electron 或基于 V8 衍生的浏览器。

于 2021 年 4 月 13 日曝光的 CVE-2021-21220 Chrome 远程代码执行漏洞，Chrome 中的 V8 引擎的 JIT 编译器中对 JavaScript 优化时存在远程代码执行漏洞，攻击者可以构造特殊网页插入恶意 JS 代码，利用水坑攻击诱使受害者使用 Chrome 访问攻击者的恶意网站，触发漏洞，从而在受害者电脑上远程执行代码。该漏洞细节及分析在互联网上公开，随后在 8 月份 msf 增加了该漏洞的利用模块。在 2021 年，此类利用浏览器漏洞进行攻击的事件相比于往年增加了不少，且被 APT 组织利用的漏洞大多“品相”不错，容易稳定利用。在 CVE-2021-21220 曝光同月 21 日，Chrome 又被曝出 APT 在野利用漏洞 CVE-2021-21224，APT 组织 PuzzleMaker 在针对多家公司的 APT 攻击中串联使用了 Chrome 远程代码执行漏洞 CVE-2021-21224 和 Windows10 内核提权漏洞 CVE-2021-31956，通过组合利用两个漏洞，攻击者成功在目标机器上远程执行代码。

2021 年 9 月 13 日，谷歌发布 Chrome 93.0.4577.82 版本，在版本更新日志中指出由匿名安全研究人员报告的漏洞 CVE-2021-30632 和 CVE-2021-30633 正在被广泛利用,CVE-2021-30632 是 Chrome 的 JIT 编译器中的一个类型混淆错误，攻击者可以构造恶意 JavaScript 代码插入到恶意网站中，诱使受害者通过 Chrome 访问即可导致 Chrome 渲染进程远程执行代码,CVE-2021-30633 是 Chrome 的 IndexedDB API 中的一个释放后使用漏洞，可以配合 CVE-2021-30632 进行沙箱逃逸，通过组合利用这两个漏洞，攻击者可以完全控制 Chrome。

在 2021 年 9 月 30 日，谷歌发布了 Chrome 更新，修复了在野利用漏洞 cve-2021-37975 Chrome 远程代码执行漏洞和 cve-2021-37976 Chrome 信息泄露漏洞，在 cve-2021-37975 中主动触发了 V8 引擎的垃圾收集器（GC），V8 引擎的 GC 对 JavaScript 对象进行回收，但该对象仍然在 JavaScript 代码中存在引用，由此造成了释放后重用，利用释放后重用进一步造成远程代码执行。攻击者可以构造特殊页面，插入恶意 JS 代码，诱使受害者访问该页面即可达到远程代码执行，谷歌在 Chrome 更新日志特别指出 cve-2021-37975 和 cve-2021-37976 存在在野利用。

- Atlassian Confluence

Atlassian Confluence（简称 Confluence）是一个专业的企业知识管理与协同软件，并支持用于构建企业 WiKi，通过它可以实现团队成员之间的协作以及知识共享。

2021 年 8 月 25 日，Atlassian 官方发布 Atlassian Confluence Server OGNL 表达式注入漏洞通告（CVE-2021-26084），经过身份验证的远程攻击者（在某些场景下无需身份验证）可注入 OGNL 表达式从而在系统上执行代码。2021 年 8 月 31 日，该漏洞的利用细节及演示视频在互联网上公开，指出利用该漏洞无需身份认证，默认配置下，攻击者通过在特定路由的 tag 标签中插入 OGNL 表达式即可远程执行代码。2021 年 9 月 1 日，Bad Packets 发现了大规模针对该漏洞的扫描活动，开始扫描互联网上易受漏洞影响的系统。2021 年 9 月 4 日，Atlassian 官方修改通告申明利用此漏洞无需身份认证，并已检测到在野利用。

Atlassian JIRA 是 Atlassian 公司出品的项目与事务跟踪工具，被广泛应

用于缺陷跟踪、客户服务、需求收集、流程审批、任务跟踪、项目跟踪和敏捷管理等工作领域。多部署于企业内网，采用 Java 开发。

2021 年 7 月 21 日，Atlassian 官方发布 Jira Data Center 和 Jira Service Management Data Center 远程代码执行漏洞通告（CVE-2020-36239）。该漏洞与 Jira Data Center 等产品中使用的 Ehcache 开源组件所支持的 RMI 服务相关，远程攻击者无需身份认证即可向 RMI 端口发送特制请求来触发反序列化漏洞，最终导致任意代码执行。该产品存在约 1.8w 客户使用，而这些客户均处在这个高危漏洞的威胁中。

- GitLab

GitLab 是一款开源的 Git 仓库管理工具，2021 年 10 月 25 日，奇安信 CERT 监测到 GitLab CE 远程命令执行漏洞(CVE-2021-22205)在野利用事件在互联网上传播，并且该事件公开披露了漏洞利用细节，未经身份验证的攻击者可以在受害者服务器上执行任意代码。

Gitlab 作为企业中最常用的 git 仓库管理工具之一，一旦爆发漏洞，那么暴露在公网上的 gitlab 服务器是非常危险的，攻击者能够利用该漏洞实施勒索攻击、构建僵尸网络、种植挖矿木马等恶意操作，这给企业带来的损失是无法估计的，但是值得注意的是，该漏洞早在 2021 年 4 月 7 日进行了公开，2021 年 4 月 17 日进行了修复，直到 2021 年 10 月 25 日在野利用事件公开之后，各大厂商才开始重视起来，这也再次给企业的安全问题敲响了警钟，企业不重视安全问题，不关注开源项目的安全更新，这才导致了后续的危害，若企业能够早日更新 GitLab 版本，早日修复漏洞，那么漏洞利用工具公开后也不会受到影响。

- Exim

Exim 是由英国剑桥大学的 Philip Hazel 基于 GPL 协议开发的消息传输代理（Message Transfer Agent，MTA）负责邮件的路由、转发和投递，运行于类 Unix 系统上。Exim 和其他 MTA 相比最大的特点是灵活性高、拓展性好，Exim 的配置文件是一个文本文件，支持通过 String Expansion 技术定义配置。String Expansion 是一种简单的脚本语言，能够实现定义变量、条件判断、字符串转换

等功能，截至本文撰写时 Exim 最新版本为 4.95。

2021 年 Exim 总共产生 22 个 CVE，包含了 2021 年 5 月份来自 Qualys 的国外安全研究员披露的 21 个 Exim 漏洞，Qualys 披露的漏洞中部分影响 2004 年到 2021 年 5 月份内的所有 Exim 版本。

在 2021 年 5 月份公布的安全报告中包含 21 个 Exim 漏洞，可以分为本地利用类漏洞和远程利用类漏洞，可以远程利用的漏洞中比较值得注意的是 CVE-2020-28018、CVE-2020-28020 和 CVE-2020-28024。在基于 OpenSSL 构建的 Exim 中，未授权的攻击者可以利用 CVE-2020-28018 Exim 释放后重用漏洞的任意读读取 Exim 进程堆内敏感信息，之后利用该漏洞的任意写在 Exim 进程的特殊内存位置内写入恶意命令，利用 Exim 的功能特性，攻击者即可以在服务器上远程执行命令，该漏洞细节已在报告中公开，在 5 月 14 号国外安全研究员对该漏洞进行了深入分析，随后在该漏洞的 PoC 公开在 Github 上。第二个漏洞是 CVE-2020-28020，在 Exim 中的 receive_msg()函数允许攻击者实现从整数溢出到缓冲区溢出，未授权的攻击者可以利用该漏洞在 Exim 的上下文以 Exim 用户身份执行代码，或者利用该漏洞让 Exim 进程崩溃造成拒绝服务，该漏洞影响 4.92 之前的所有 Exim 版本，该漏洞细节和造成拒绝服务的 PoC 已在 Qualys 的漏洞报告中公开。

可以本地利用的漏洞中值得关注的是 CVE-2020-28007、CVE-2020-28008 和 CVE-2020-28023。 由于 Exim 在日志目录（由非 root 用户拥有）中以 root 身份运行。通过利用 CVE-2020-28007 攻击者可以使用符号链接或硬链接攻击覆盖系统上任何地方的 root 用户的文件。攻击者可以利用该漏洞覆盖/etc/passwd 文件，将自身权限提升至 root。CVE-2020-28008 Exim 命令执行漏洞形成原因和 CVE-2020-28007 类似，Exim 在 spool 目录（由非 root 用户拥有）中以 root 权限运行，攻击者可以在 /var/spool/exim4/input spool 头文件中写入特殊的收件人地址，从而间接导致缓冲区溢出或命令执行。以上漏洞细节、PoC 均已被国外安全研究员公开。

3. 漏洞情报展望

3.1 为什么我们需要漏洞情报？

从企业的角度来看，没有一种方法能够保证业务系统绝对安全。由于企业对风险管理的要求较高，仅仅做脆弱性管理无法满足企业控制信息风险的需求。企业的安全建设只有防御远远不够，还需要持续地检测与响应，而要做到更有效的检测与更快速的响应，安全情报必不可少。在网络空间的广度和深度不断拓展、安全对抗日趋激烈的今天，安全情报已经成为了企业控制风险的一种重要手段。

威胁情报和漏洞情报作为安全情报大家族中的“大哥”和“二哥”，近年来已经成为了国内外安全领域的热点。威胁情报描述现存的、或者是即将出现的针对资产的威胁，可用于通知主体针对相关威胁采取某种响应。漏洞情报帮助企业漏洞管理者迅速判别漏洞对企业业务的影响，让管理者能够第一时间进行漏洞处置，避免后续风险的扩散。获取威胁情报是为了“知彼”，获取漏洞情报是为了“知己”，《孙子兵法·谋攻篇》有言：“知己知彼，百战不殆。”

3.2 好的漏洞情报应该提供哪些价值？

基于奇安信 CERT 的漏洞情报运营实践，我们认为漏洞情报的运营需要起到收集器、过滤器和富化器的作用。通过对一手数据源的挖掘和信息实时采集，结合威胁情报对漏洞进行多维度的属性标定，保证漏洞情报的全面性和及时性；分析团队依据完善的流程和专业经验对漏洞的影响面和技术细节进行研判，把真正重要的漏洞过滤出来，保证信息的准确性和处理优先级的可靠性；对于确认的重要漏洞，好的漏洞情报需要给出切实可行的处理方法，提供除补丁链接以外的其他威胁缓解措施，富化漏洞信息的上下文。由此，我们关注漏洞情报的全面性、及时性、准确性、可靠性和可行性（如图 3-1），下面是一些具体的运营目标和实践。

图 3-1 漏洞情报评判标准

3.2.1 全面的多维漏洞信息整合及属性标定

一般的漏洞库的核心信息只会涉及软硬件影响面（厂商、应用及版本）和漏洞本身技术层面的评估（威胁类型、利用场景、危害大小等），这只能让我们对漏洞本身的属性有个基本的了解。但是为了有效管控漏洞导致的风险，我们需要知道得更多：

- 漏洞是否在默认配置下存在，配置情况对漏洞可利用性影响极大，非默认配置下的漏洞其实际威胁往往远不如技术层面看起来那么大
- 漏洞相关的应用系统部署量有多大，这直接影响漏洞整体的威胁评估
- 漏洞是否已经有了公开的技术细节、Exploit 工具、概念验证代码（PoC），这也会间接影响漏洞转变为现实的攻击
- 漏洞是否已经有了野外的利用，这体现了漏洞是否已经从潜在威胁转化为了现实威胁
- 漏洞是否已经被已知的漏洞利用攻击包或大型的 Botnet 集成作为获取

对系统控制的途径

- 漏洞是否为 0day 或 APT 活动相关，意味着漏洞可能被用于攻击高价值的目标

所有上面这些都应该通过运营被标记出来，以方便用户进行有效的处理优先级排序。

图 3-2 是我们对 2021 年底核弹级漏洞 Apache Log4j 任意代码执行漏洞(CVE-2021-44228)[12]的标签实例：

图 3-2 Apache Log4j 任意代码执行漏洞(CVE-2021-44228)标签实例

奇安信 CERT 的漏洞情报还会支持基于标签的搜索，让用户非常方便地获取满足特定属性的漏洞集合。

当然，上面所有的一切都是建立在全面收集漏洞信息的基础上，我们监测了多个主流漏洞数据库以及数十安全厂商,关注了 2000+推特账号和 80+安全相关新闻源，开源信息采集结合商业数据采购，并通过各种手段挖掘新的数据源。

3.2.2 及时的与组织自身相关漏洞风险通知

目前从漏洞信息公开到野外实际利用攻击出现的间隔期越来越短，大多数时

12 https://nox.qianxin.com/vulnerability/detail/QVD-2021-35958

候防御方是在跟攻击者抢时间，哪方先知道漏洞的存在及相应的细节决定了谁在对抗中获胜。为了及时输出漏洞风险通知，漏洞情报的运营理想条件下需要采用 7*24 的监测处理机制，直接的厂商源头信息采集，及时研判并实时推送漏洞状态更新。奇安信 CERT 认为如下 5 类漏洞相关的状态更新需要尽快推送给我们的用户，因为这些更新会直接影响漏洞在现实世界的危害程度：

- 新的关键漏洞公开
- 发现关键漏洞的技术细节
- 发现关键漏洞的 Exploit 或 PoC 公开
- 发现关键漏洞的在野利用案例
- 发现关键漏洞的新修补和缓解方案

为了尽快触达用户提供尽可能快的信息推送，我们创建了直达用户的微信群，图 3-3 是我们在试运行过程中推送的微信群消息实例。

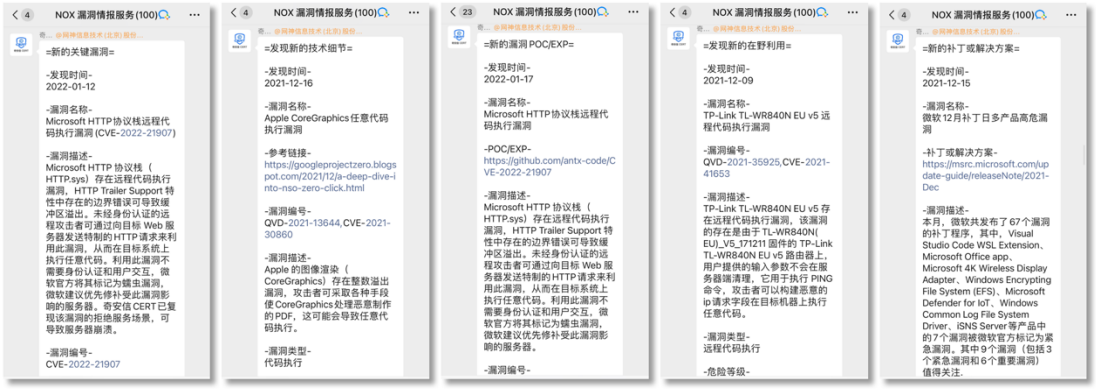

图 3-3 微信群消息推送实例

我们的微信群二维码如下，此群只会推送经过奇安信 CERT 团队验证过的有现实威胁的漏洞信息，免费社区，欢迎加入。

NOX 漏洞情报服务微信群入群二维码

2021 年奇安信 CERT 发布了涉及 40 多个重点厂商、300 余条漏洞的 147 篇实时安全风险通告[13]。其中 CVE-2021-21224 Google Chrome 远程代码执行漏洞（发现时漏洞为 0day 状态）、WebLogic T3 反序列化 0day 漏洞、CVE-2021-28474 Microsoft SharePoint 远程代码执行漏洞等漏洞的风险通告均为奇安信 CERT 团队使用自研 PoC 首次验证并第一时间发布的安全风险通告。

为了能让组织全面地获取自身网络环境相关的漏洞信息，我们引入了全面的 CPE 信息集成，非 CVE 漏洞（主要是国产软件漏洞）的扩展 CPE 支持，使用归一化的厂商及产品列表，包含 1000+软件厂商、10000+产品，精准定位漏洞影响面，第一时间提供高危漏洞定向风险通告，后续还会提供基于受影响软件筛选的定制漏洞情报输出。

3.2.3 准确的漏洞所导致实际安全风险判定

每天平均都有几十个漏洞被公开出来，对其进行全部的分析验证需要巨量的资源，对任何厂商和组织都是不可能完成的任务，奇安信 CERT 设计了专门流程根据漏洞的影响面和验证条件筛选出值得深入分析的漏洞，多种渠道收集或自研 PoC 进行技术验证。这是一项在漏洞情报运营过程中专业度要求最高的环节，团队在这方面有人员投入，保证我们对于重要漏洞在技术层面有完整的理解，对外

13 https://nox.qianxin.com/risk

输出对于漏洞最权威的意见。

在 2021 年，Microsoft Windows Active Directory 域服务特权提升漏洞（CVE-2021-42287）[14]、Apache APISIX Dashboard 未授权访问漏洞（CVE-2021-45232）[15]、Grafana 未授权任意文件读取漏洞（CVE-2021-43798）[16]等漏洞经过 NOX 安全监测平台的专业漏洞分析团队（奇安信 CERT）复现并被打上“奇安信 CERT 验证”标签，标记我们对于此类严重漏洞的存在性和可利用性的专业验证。

对于漏洞技术细节的深入理解使我们真正把需要重点关注处置的漏洞从海量几乎没什么实际风险的漏洞中挑选出来，漏洞运营的目标也不仅仅告诉用户哪些漏洞重要，同样重要的，告诉用户哪些漏洞所对应风险名不副实。一个典型的例子是 2021 年 12 月 Log4j 漏洞爆发以后，由于聚光灯效应，一些衍生漏洞随之出现，团队对那些漏洞研究分析之后确认其中绝大部分并没有实际场景下的威胁，随即发布了相关的风险通告做了技术上的澄清。图 3-4 是奇安信 CERT 所发布澄清报告的例子：

图 3-4 奇安信 CERT 发布的澄清报告

3.2.4 可靠的综合性漏洞处理的优先级排序

14 https://nox.qianxin.com/vulnerability/detail/QVD-2021-35959
15 https://nox.qianxin.com/vulnerability/detail/QVD-2021-36132
16 https://nox.qianxin.com/vulnerability/detail/QVD-2021-35950

面对互联网上每日出现的大量新增漏洞，大量的漏洞具有相同的 CVSS 评分，仅基于这些评分基本上很难对漏洞的实际风险做出有效的评估，其他诸如漏洞是否默认配置受影响、利用的易用性稳定性、攻击者所能接触到的存在漏洞的资产量级及漏洞利用的其他前置条件都对漏洞的实际风险有极大影响，而这些维度的评价在 CVSS 评分体系中非常难以准确量化。

目前普遍基于 CVSS 评分的高低来评估漏洞的危险程度，但这样真的能准确地反映漏洞的实际风险吗？我们对于数据库的数据做了简单的分析，CVSS 评分高于 9.0 的漏洞数量有 13000 多个，其中有 3300（25%）多个漏洞存在对应的 Exploit，这个比例不算低，但只有 580 多个漏洞被标记存在野外利用，占比这类高危漏洞不到 5%的比例。所以，即便是技术层面风险度非常高的漏洞，真正被利用来攻击造成威胁的概率也不高。

从以上的数据分析可以看到，相同的 CVSS 评分大概率并不具有相同的实际风险。同样 CVSS3 10 分的漏洞，就仅在易用性稳定性上的差异，就会使 Log4j 这样顶级漏洞与其他同样 10 分漏洞在实际威胁上判若云泥。这个难题需要通过结合威胁情报来缓解，奇安信 CERT 的漏洞情报多维度标签为用户提供了基于漏洞现时状态进行优先级排序的可能。

NOX 安全监测平台现已收录关键漏洞 18180 个[17]，并将漏洞按照更新时间先后进行排序，例如：该页面中 Apache Log4j 任意代码执行漏洞(CVE-2021-44228)、Google Chrome 远程代码执行漏洞(CVE-2021-37973)、致远 OA 代码执行漏洞(CNVD-2021-51370)等漏洞已经被标注为“发现在野利用”并且漏洞威胁等级为“高危”或“极危”，此类漏洞建议用户参考漏洞的详情页面给出的漏洞修补方法尽快进行修补。

我们将已经存在野外利用的、已有公开 Exploit/PoC、已有技术细节的高危漏洞圈定为关键漏洞，对此类漏洞做重点运营。随本报告同时发布还有已确认存在野外利用的漏洞列表（附录 1），这类已经导致现实安全风险的漏洞应该成为每一个认真对待漏洞威胁的组织的必修对象。

17 https://nox.qianxin.com/KeyPoint

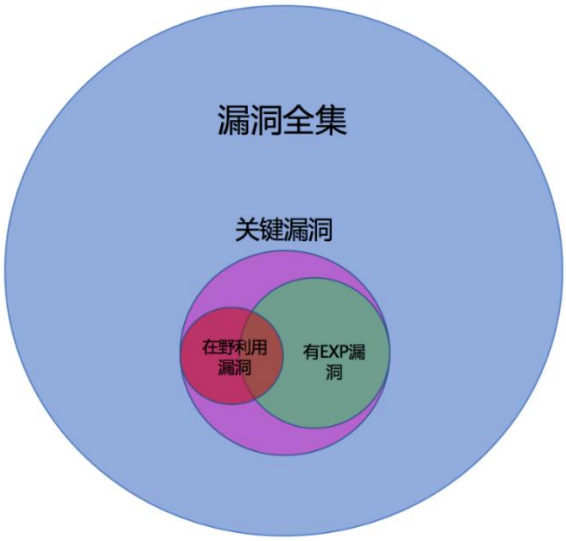

图 3-5 关键漏洞图示

3.2.5 可行的包含详细操作步骤的处置措施

除了全面性、及时性、有效性，提供有效的缓解措施和可落地解决方案也是漏洞情报实现其价值的重要一环，仅有补丁链接在很多场景下是远远不够的，因为打补丁受各种现实条件的限制，比如重要服务器出于性能和稳定性的考虑没有经过完整的补丁测试是不让随便打补丁的，有些补丁打完以后需要重启机器的操作是不允许的，更不用提 0day 漏洞暂时无补丁可打的情况。对于很多重要漏洞，奇安信 CERT 团队还会组织能力部门和产品开发主机或网络虚拟补丁，寻找通过配置暂时规避漏洞利用的临时解决方案，通过经验证的 step-by-step 的操作步骤，帮助系统管理员迅速上手进行漏洞处置。

例如：对于 ProxyLogon 漏洞，NOX 安全监测平台持续更新 6 次安全风险通告，不断对缓解措施进行完善，最终提供了两千余字详细描述的可行操作步骤。对于 Log4Shell 漏洞，NOX 安全监测平台给出的完整处置建议涵盖了漏洞排查、攻击排查、修复版本、产品解决方案以及多种不同场景下经过验证的有效缓解措施，该完整的处置建议在奇安信多家客户单位的一线应急响应中做出了重大贡献。

3.3 个人、企业、安全监管单位如何选择优质的漏洞情报？

当前的网络安全正处在一个转型升级的上升期，网络安全体系架构已经由基

础架构安全、被动防御向主动防御、反制进攻阶段进化。传统的安全思维模式和安全技术已经无法有效满足政企客户对安全防护的需要，新的安全理念、新的安全技术不断涌现。要实现有效的积极防御，很关键的一点是要具备安全情报的发现与使用能力。

对于个人用户、企业用户以及安全监管单位而言如何挑选到满足自身业务需求的优质漏洞情报，可以简单概括为一句话:“C 端用户挑产品、B 端用户挑服务、监管机构挑供应商”。个人用户只需要确保自身的隐私安全和资产安全，不需要关注漏洞本身的技术细节，因此在漏洞情报的使用上更加依赖于其部署的终端安全产品对漏洞情报的敏感程度；企业用户基于其信息系统的复杂程度，单一的安全产品无法满足其建立企业自身漏洞检测与响应能力的需求，企业需要更加精准和定制化的漏洞情报服务，来帮助管理者迅速判别漏洞对企业业务的影响，并第一时间进行有效的漏洞处置；安全监管单位关注全网的网络安全态势，需要庞大的漏洞情报数据库支撑，更加考验漏洞情报供应商在模式化的安全产品和情报服务之上，所拥有的灵活、可变通的业务适应能力。

奇安信 CERT NOX 平台和团队运营的漏洞情报服务可以是一个值得了解和评估的选项，欢迎访问我们的网站 https://nox.qianxin.com/vulnerability 查看我们的运营成果，有需要的话可以进一步合作。

附录 1：历年在野利用漏洞列表

序号	QVD ID	CVE ID	公开日期	漏洞类型	漏洞名称	涉及厂商	涉及产品
1	QVD-2021-18883	CVE-2021-35247	2022-01-10	安全特性绕过	Solarwinds Serv-U 输入验证错误漏洞(CVE-	SOLARWINDS	Solarwinds Serv-U
2	QVD-2021-35963	CVE-2021-44168	2022-01-04	文件读取	Fortinet FortiOS 任意文件	FORTINET	Fortinet FortiOS
3	QVD-2013-6317	CVE-2013-3307	2021-12-30	内存损坏	Linksys X3000 缓冲区溢出漏洞(CVE-2013-3307)	LINKSYS	Linksys X3000
4	QVD-2021-13068	暂无	2021-12-28	代码执行	致远OA远程代码执行漏洞(CNVD-2021-51370)	北京致远互联软件股份有限公司	A8+,A6+,G6
5	QVD-2021-36132	CVE-2021-45232	2021-12-27	错误的访问控制	Apache APISIX Dashboard 未授权访问漏洞	APACHE	APISIX Dashboard
6	QVD-2020-78239	CVE-2021-1048	2021-12-15	权限提升	Google Android 权限提升漏洞(CVE-2021-1048)	GOOGLE	Chrome
7	QVD-2021-36056	CVE-2021-43890	2021-12-15	代码执行	Microsfot Windows AppX Installer 欺骗漏	MICROSOFT	App Installer
8	QVD-2021-36057	CVE-2021-43883	2021-12-15	权限提升	Microsfot Windows Installer 权限提升漏洞(CVE-2021-	MICROSOFT	Windows
9	QVD-2021-36058	CVE-2021-45046	2021-12-14	远程代码执行	Log4j 远程代码执行漏洞(CVE-2021-45046)	APACHE	Log4j
10	QVD-2021-36137	CVE-2021-4102	2021-12-14	释放后重用	Google Chrome 释放后重用漏洞 CVE-2021-4102	GOOGLE	Chrome
…	…	…	…	…	…	…	…

历年在野利用漏洞完整列表，请到以下链接下载：

https://oss-sh-shyc3.yun.qianxin.com:443/nox-file/%E9%99%84%E5%BD%951%EF%BC%9A%E5%8E%86%E5%B9%B4%E5%9C%A8%E9%87%8E%E5%88%A9%E7%94%A8%E6%BC%8F%E6%B4%9E%E5%88%97%E8%A1%A8.xlsx?AWSAccessKeyId=BBBUJ0KKK9C03PWDPGCH&Signature=lx4PVWe2POTSG25uGGAfxNVsjxk%3D&Expires=1676359351

当前列表收录漏洞 3923 个，列表每日持续更新！

附录 2：2021 年度 APT 活动相关漏洞列表

漏洞编号	影响目标	利用代码是否公开	利用的 APT 组织	披露厂商	攻击事件披露
CVE-2020-11261	Android	是	未知	未知	未知
CVE-2021-1647	Windows Defender	是	未知	未知	未知
CVE-2021-1782	IOS	否	未知	未知	未知
CVE-2021-1870	IOS	否	未知	未知	未知
CVE-2021-1871	IOS	否	未知	未知	未知
CVE-2021-21148	Chrome	否	Lazaurs 针对安全研究人员的定向攻击	未知	未知
CVE-2021-21017	Adobe Reader	否	未知	未知	未知
CVE-2021-1732	Windows	是	BITTER 通过 Windows 提权 0day 攻击中国重点单位	安恒	https://ti.dbappsecurity.com.cn/blog/index.php/2021/02/10/windows-kernel-zero-day-exploit-is-used-by-bitter-apt-in-targeted-attack/
CVE-2021-26855	Exchange Server	是	未知	Volexity/DEVCORE/Microsoft Threat Intelligence Center	https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
CVE-2021-26857	Exchange Server	否	未知	Volexity/DEVCORE/Microsoft Threat Intelligence Center	https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
CVE-2021-26858	Exchange Server	否	未知	Volexity/DEVCORE/Microsoft Threat Intelligence Center	https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

CVE-2021-27065	Exchange Server	是	未知	Volexity/DEVCORE/Microsoft Threat Intelligence Center	https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
CVE-2021-21166	Chrome	否	未知(针对亚美尼亚的定向攻击事件)	Microsoft Browser Vulnerability Research	https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/
CVE-2021-26411	Internet Explorer	是	Lazaurs 针对安全研究人员的定向攻击	Enki/360	https://enki.co.kr/blog/2021/02/04/ie_0day.html
CVE-2021-21193	Chrome	否	未知	未知	
CVE-2021-1879	IOS	否	APT29 针对西欧政府官员的定向攻击事件	Google Threat Analysis Group	https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/
CVE-2021-28310	Windows	否	BITTER Windows 提权 0day 攻击事件	Kaspersky	https://securelist.com/zero-day-vulnerability-in-desktop-window-manager-cve-2021-28310-used-in-the-wild/101898/
CVE-2021-21220	Chrome	是	无	自由安全研究人员	未知
CVE-2021-21224	Chrome	是	无	360	未知
CVE-2021-22893	Pulse Secure VPN	否	UNC2630 针对美国国防工业基地(DIB) 网络攻击	FireEye	https://www.mandiant.com/resources/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day
CVE-2021-20021	SonicWall	否	UNC2682	FireEye	https://www.mandiant.com/resources/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise
CVE-2021-20022	SonicWall	否	UNC2682	FireEye	https://www.mandiant.com/resources/zero-day-exploits-in-sonicwall-

					email-security-lead-to-compromise
CVE-2021-20023	SonicWall	否	UNC2682	FireEye	https://www.mandiant.com/resources/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise
CVE-2021-27059	Office	否	未知	FireEye	未知
CVE-2021-27085	Internet Explorer	否	未知	FireEye	未知
CVE-2021-28550	Adobe Reader	否	未知	未知	未知
CVE-2021-30551	Chrome	否	未知(针对亚美尼亚的定向攻击事件)	Google's Threat Analysis Group and Google Project Zero	https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/
CVE-2021-30661	WebKit	否	未知	360	未知
CVE-2021-30663	WebKit	否	未知	未知	未知
CVE-2021-30665	WebKit	否	未知	360	未知
CVE-2021-30666	WebKit	否	未知	360	未知
CVE-2021-30761	WebKit	否	未知	未知	未知
CVE-2021-30762	WebKit	否	未知	未知	未知
CVE-2021-1905	Android	否	未知	未知	未知
CVE-2021-1906	Android	否	未知	未知	未知
CVE-2021-28663	Android	否	未知	未知	未知
CVE-2021-28664	Android	否	未知	未知	未知
CVE-2021-31199	Winodws	否	未知	未知	未知
CVE-2021-31201	Winodws	否	未知	未知	未知
CVE-2021-31955	Winodws	否	PUZZLEMAKER 通过	Kaspersky	https://securelist.com/puzzlemaker-chrome-

			Chrome 攻击链完成的定向攻击事件		zero-day-exploit-chain/102771/
CVE-2021-31956	Winodws	否	PUZZLEMAKER 通过 Chrome 攻击链完成的定向攻击事件	Kaspersky	https://securelist.com/puzzlemaker-chrome-zero-day-exploit-chain/102771/
CVE-2021-33739	Windows	是	未知	安恒	未知
CVE-2021-33742	Internet Explorer	否	未知(针对亚美尼亚的定向攻击事件)	Google’s Threat Analysis Group	https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/
CVE-2021-30554	Chrome	否	未知	未知	未知
CVE-2021-33771	Windows	否	SOURGUMto 通过 Windows 提权 0day 攻击巴勒斯坦权力机构	未知	https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/
CVE-2021-34448	Internet Explorer	未知	未知	360	未知
CVE-2021-31979	Windows	否	SOURGUM 通过 Windows 提权 0day 攻击巴勒斯坦权力机构	Microsoft Threat Intelligence Center (MSTIC)/ Microsoft Security Response Center (MSRC)	https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/
CVE-2021-30563	Chrome	否	未知	未知	未知
CVE-2021-30807	IOS	否	未知	未知	未知
CVE-2021-36948	Windows	否	未知	未知	未知
CVE-2021-1675	Windows printer	是	未知	Tencent Security Xuanwu Lab/AFINE/NSFOCUS	未知

CVE-2021-34527	Windows printer	是	未知	未知	未知
CVE-2021-36936	Windows printer	是	未知	未知	未知
CVE-2021-36958	Windows printer	是	未知	未知	未知
CVE-2021-40444	Internet Explorer	是	未知	Rick Cole (MSTIC), Dhanesh Kizhakkinan of Mandiant, Genwei Jiang of Mandiant, Haifei Li of EXPMON, and Byce Abdo of Mandiant	未知
CVE-2021-30860	IOS iMessage	否	NSO	The Citizen Lab	https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
CVE-2021-30858	WebKit	否	未知	未知	未知
CVE-2021-30632	Chrome	是	未知	未知	未知
CVE-2021-30633	Chrome	否	未知	未知	未知
CVE-2021-1789	Webkit	否	未知	Google TAG/ Google Project Zero	https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/
CVE-2021-30869	macOS	否	未知	Google TAG/ Google Project Zero	https://blog.google/threat-analysis-group/analyzing-watering-hole-campaign-using-macos-exploits/
CVE-2021-37973	Chrome	否	未知	Google TAG/ Google Project Zero	未知
CVE-2021-37975	Chrome	是	未知	未知	未知

CVE-2021-37976	Chrome	是	未知	Google TAG/ Google Project Zero	未知
CVE-2021-30883	IOS	否	未知	未知	未知
CVE-2021-40449	Windows	是	MYSTERYSNAIL	Kaspersky	未知
CVE-2021-38000	Chrome	否	未知	Google TAG/ Google Project Zero	未知
CVE-2021-38003	Chrome	否	未知	Google TAG/ Google Project Zero	未知
CVE-2021-1048	Android	否	未知	未知	未知
CVE-2021-42292	Office	否	未知	Microsoft Threat Intelligence Center (MSTIC)	未知
CVE-2021-42321	Exchange	是	未知	Microsoft Security Response Center/Microsoft Threat Intelligence Center (MSTIC)/360	未知
CVE-2021-40539	Zoho ManageEngine ADSelfService	是	APT27	未知	https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/
CVE-2021-22005	VMware vCenter Server	是	OceanLotus	未知	未知
CVE-2021-44228	Apache Log4j	是	未知	未知	未知
CVE-2021-4102	CHROME	是	未知	未知	未知
CVE-2021-42287	Windows Active Directory	是	未知	未知	未知
CVE-2021-42278	Windows Active Directory	是	未知	未知	未知

感谢以下人员对本报告的贡献：

汪列军、谷亮、郝桐彤、王淋、Strawberry、medi0cr1ty、Cherry可可、Veraxy、s0xzordIn

联系我们：

WeChat：QAX_CERT

Mail:cert@qianxin.com