奇安信
威胁情报中心

漏洞态势

全网漏洞态势研究报告

2023年度报告

2024年1月

关键词：漏洞事件、勒索攻击、关键漏洞、APT相关

主要观点 MAIN POINTS

过去一年，奇安信漏洞情报，聚焦国内外新增高危漏洞，迅速响应、权威研判、持续跟踪。已经形成一套完整的漏洞情报供应体系，帮助企业前置漏洞处置流程、及时发现漏洞风险、修复潜在威胁，构建更加完善的安全防护能力。

《2023年全网漏洞态势研究报告》从漏洞视角出发，观察2023年网络安全现状，梳理全年整体漏洞态势、盘点和分析漏洞利用相关的安全事件以及有现实威胁的关键漏洞。核心洞见如下：

- 2023年公开漏洞的总数持续上升，类型分布与往年类似，导致实际安全风险的漏洞比例并没有增加，我们还是应该通过威胁情报及时发现那些关键漏洞，以最快的速度加以处置。

- APT组织利用了不少高端0day漏洞执行高度定向的攻击，甚至在卡巴斯基揭露的三角行动中使用了非常罕见的硬件漏洞。这些漏洞的利用基本上是无法防御的，对于敏感的人员和机构使用可信可追溯的软硬件进行工作必须成为一个认真考虑的选项。

- 当前定向勒索攻击活动对于政企机构的数据安全构成巨大的威胁，甚至比APT活动更甚，因为勒索攻击会直接影响业务的连续性，造成非常大的外部影响。1day/Nday漏洞的快速利用是黑产活动的最主要渗透入口之一，特别是那些涉及软硬件流行面很广而又利用稳定的场景，几乎必然会被勒索黑产大规模利用，对于影响面大而又稳定的漏洞需要尽早发现尽早修补。

- 国产软件相关的漏洞在总体漏洞中占比不高，但由于在国内的流行度高，在国内触发的实际威胁非常明显，国产软件中的漏洞挖掘值得投入，政企机构对于所使用的软件系统最好有流程化的漏洞挖掘和分析过程，或者加入补天这样的漏洞众包响应平台，以尽可能地减少严重线上漏洞的威胁。漏洞发现这件事，如果自己不做，并不能阻止网络威胁行为体去做，后果就是自己失陷而不自知。

- 有50%左右发现在野利用的0day漏洞没有监测到公开的利用代码，处于私有状态，仅被某些APT组织或者个人使用，可能用于高度定向、高价值目标、隐蔽性和供应链等攻击。所以，仅仅通过事后打补丁或采取临时规避措施很难甚至解决大部分问题，组织需要采取综合的安全措施，包括削减攻击面、威胁情报共享、安全意识培训等，以应对这些未公开的漏洞利用。

- 已知被利用的漏洞中，漏洞从公开到发现在野利用平均时间差为35天，有一半以上的漏洞在被公开后5天之内发现在野利用。显示对于大多数漏洞在公开后的短时间内就会被恶意攻击者发现并开始利用。因此，及时修补漏洞和加强网络安全措施对于保护系统和数据的安全至关重要。

- 奇安信CERT在2023年推荐必修漏洞共360个，标记了共超过4000个已发现在野利用的漏洞，这些基本是有实际安全威胁的问题，建议客户尽快参考处置建议做好自查及防护，同时通过邮件或加入微信群订阅奇安信的漏洞情报服务随时获取相关更新。

目录 CATALOGUE

01

2023年度漏洞态势

第一章

一、年度漏洞处置情况

2023年1月1日至12月31日期间，奇安信安全监测与响应中心（又称奇安信CERT）共监测到新增漏洞28975个，较2022年同比增长10.9%。其中，有7602个高危漏洞触发了人工研判。经研判：本年度值得重点关注的漏洞共793个[1]，达到奇安信CERT发布安全风险通告标准的漏洞共360个[2]，并对其中109个漏洞进行深度分析[3]。2023年奇安信CERT漏洞库每月新增漏洞信息数量如图1-1所示：

28975个
奇安信安全监测与响应中心共监测到新增漏洞

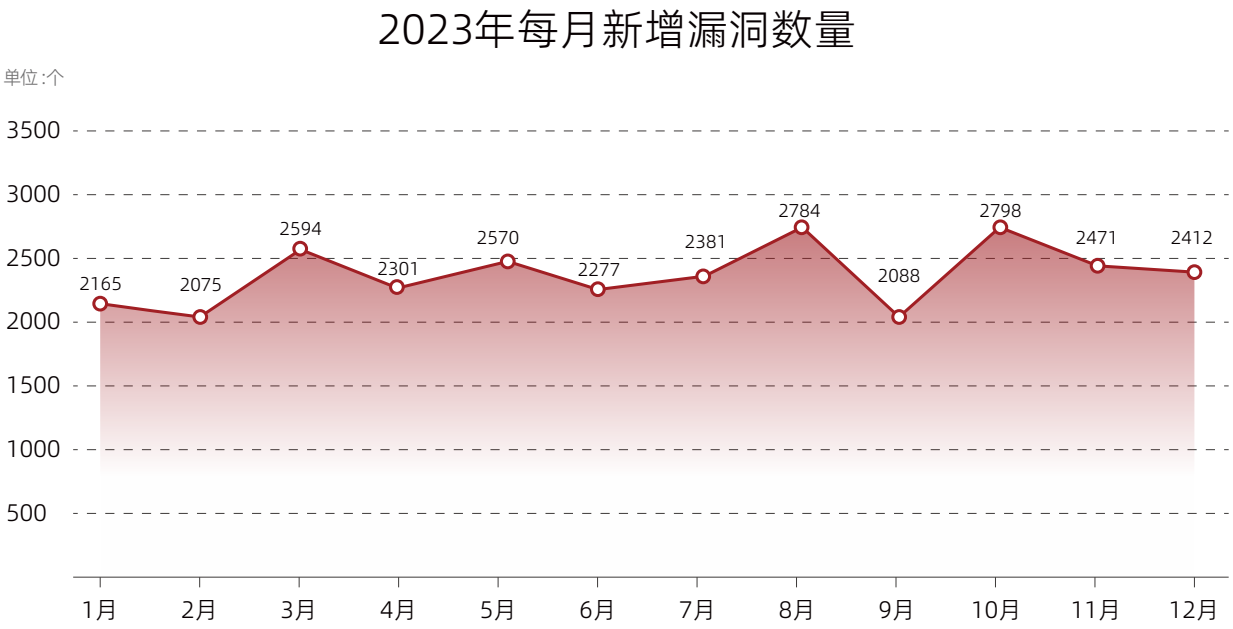
10.9%
较2022年同比增长

7602个
高危漏洞触发了人工研判

793个
本年度值得重点关注的漏洞

360个
达到奇安信CERT发布安全风险通告标准的漏洞

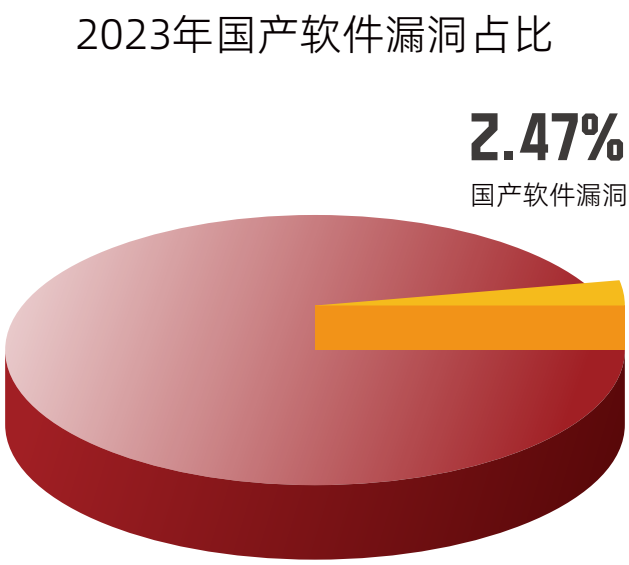
109个
漏洞进行深度分析



△图1-1 2023年奇安信CERT漏洞库每月新增漏洞信息数量

值得注意的是，2023年新增的28975个漏洞中，有715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，如果被国家背景攻击组织利用将导致严重后果。

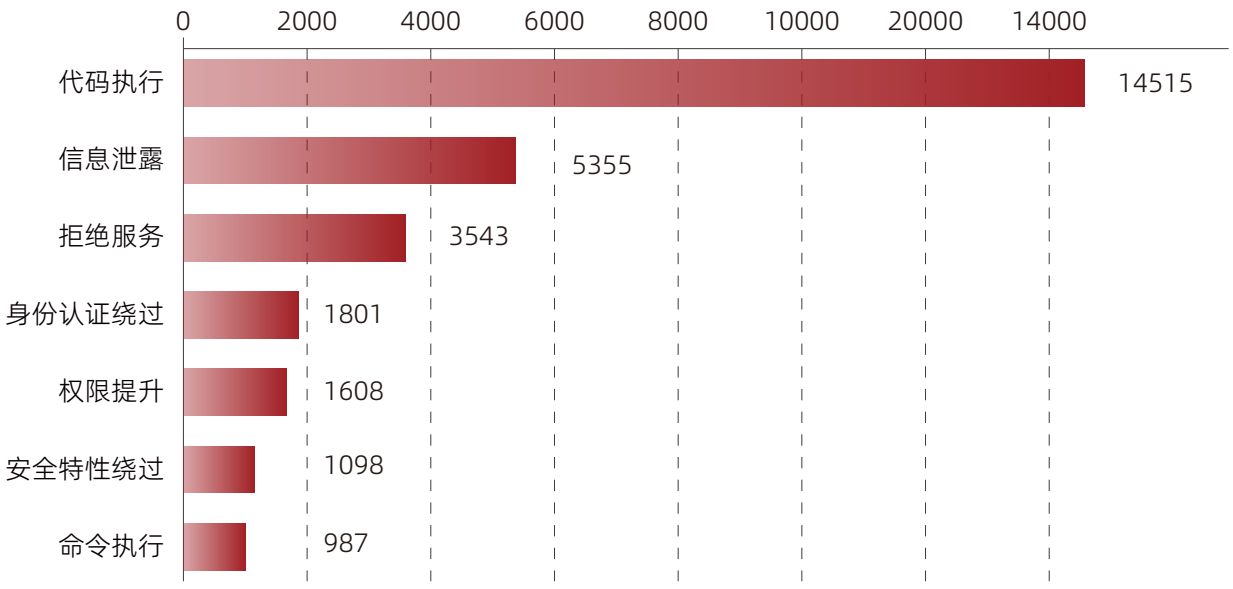
1.奇安信漏洞情报页面：https://ti.qianxin.com/vulnerability/list
2.漏洞风险通告发布页面：https://ti.qianxin.com/vulnerability/notice-list
3.漏洞深度分析报告发布页面：https://ti.qianxin.com/vulnerability/deep-analysis-report



△图1-2 国产软件漏洞占比

二、漏洞威胁类型占比情况

将2023年度新增的28975条漏洞信息根据漏洞威胁类型进行分类总结，如图1-3所示：

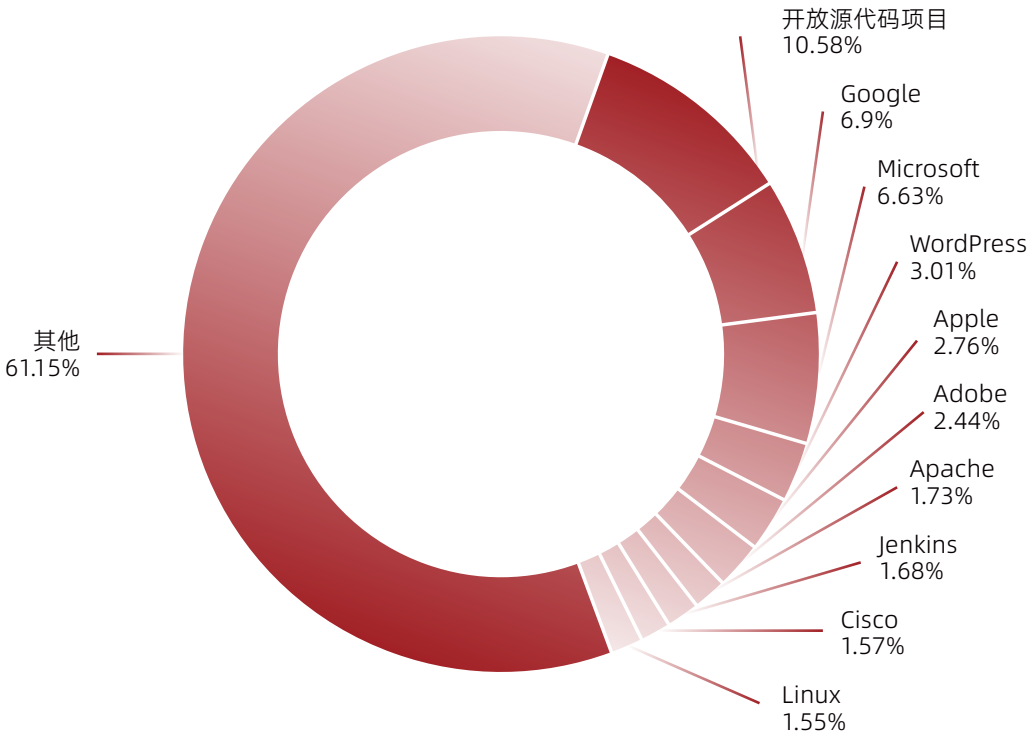


△图1-3 漏洞威胁类型排名

其中漏洞数量占比最高的前三种类型分别为：代码执行、信息泄露、拒绝服务。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。

三、漏洞影响厂商占比情况

将2023年度新增的28975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：开放源代码项目、Google、Microsoft、WordPress、Apple、Adobe、Apache、Jenkins、Cisco、Linux。Google、Microsoft、Apple这些厂商漏洞多发，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被使用的越来越多，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的重点关注。

四、漏洞威胁类型占比情况

为了更加有效的管控漏洞导致的风险，奇安信漏洞情报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”、“影响量级”、“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：

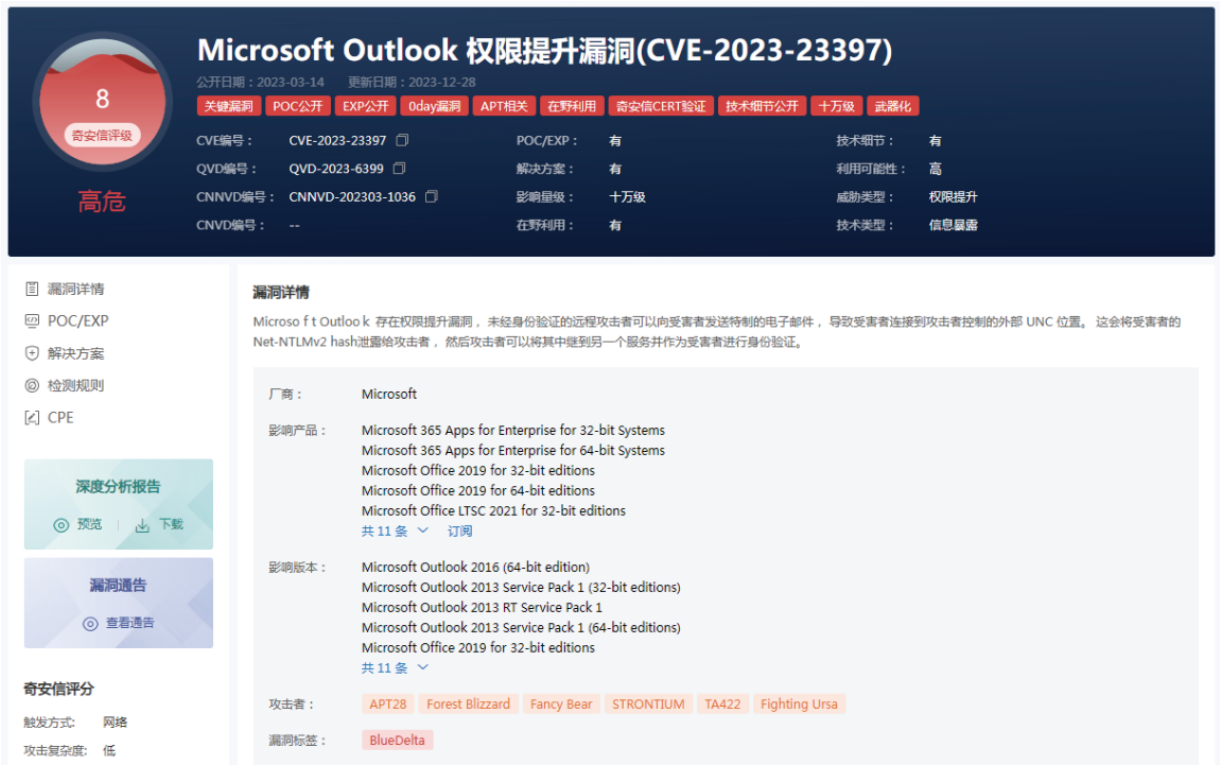
△图1-6 漏洞标签词云图

将2023年奇安信CERT人工标记的漏洞，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下表所示：

排名	漏洞名称	漏洞编号	标签数量	修复建议
1	RARLAB WinRAR 代码执行漏洞	CVE-2023-38831	28	升级至6.DEL23版本
2	Microsoft Outlook 权限提升漏洞	CVE-2023-23397	17	安装补丁
3	Apache ActiveMQ 远程代码执行漏洞	CVE-2023-46604	15	升级至安全版本
4	JetBrains TeamCity 身份认证绕过漏洞	CVE-2023-42793	14	升级至安全版本
5	Zoho ManageEngine OnPremise 多款产品远程代码执行漏洞	CVE-2022-47966	13	升级至安全版本
6	Progress MOVEit Transfer SQL 注入漏洞	CVE-2023-34362	13	升级至安全版本
7	Barracuda Email Security Gateway 远程命令注入漏洞	CVE-2023-2868	12	升级至安全版本
8	PaperCut NG和MF 身份认证绕过漏洞	CVE-2023-27350	11	升级至 MF-20.DEL1．7, DEL21.DEL2.DEL11,DEL22.DEL0.DEL9、NG-20.DEL1.DEL7,DEL21.DEL2.DEL11, 22.DEL0.DEL9版本
9	Veeam Backup & Replication 身份认证绕过漏洞	CVE-2023-27532	11	升级至安全版本
10	TP-LINK Archer AX21 代码注入漏洞	CVE-2023-1389	11	升级至安全版本

其中RARLAB WinRAR 代码执行漏洞(CVE-2023-38831)拥有的标签数量最多为28个，如图1-7所示。其次是Microsoft Outlook 权限提升漏洞(CVE-2023-23397)拥有17个标签，如图1-8所示。排名第三的Apache ActiveMQ 远程代码执行漏洞(CVE-2023-46604)被标记了15个标签，如图1-9所示。

△图1-7 CVE-2023-38831漏洞标签示例



△图1-8 CVE-2023-23397漏洞标签示例

△图1-9 CVE-2023-46604漏洞标签示例

漏洞拥有的攻击者标签越多，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。

五、漏洞热度排名TOP 10

根据奇安信CERT的监测数据，2023年漏洞舆论热度榜 TOP10漏洞如下：

排名	漏洞名称	漏洞编号	危险等级	修复建议
1	Nacos 身份认证绕过漏洞	QVD-2023-6271	高危	升级至2.2.0.1或以上版本
2	curl SOCKS5 堆溢出漏洞	CVE-2023-38545	高危	升级至8.4.0及以上版本
3	Microsoft Word 远程代码执行漏洞	CVE-2023-21716	高危	安装补丁
4	PowerShell 远程代码执行漏洞	CVE-2022-41076	高危	安装补丁
5	泛微E-Cology SQL注入漏洞	QVD-2023-15672	高危	升级至10.58及以上版本
6	Fortinet FortiOS SSL-VPN 远程代码执行漏洞	CVE-2023-27997	高危	升级至安全版本
7	Apache Kafka Connect JNDI 注入漏洞	CVE-2023-25194	高危	升级至3.4.0及以上版本
8	JumpServer未授权访问漏洞	CVE-2023-42442	高危	升级至安全版本
9	MinIO 信息泄露漏洞	CVE-2023-28432	高危	升级至RELEASE. 2023-03-20T20-16-18Z 及以上版本
10	泛微e-cology9 SQL注入漏洞	QVD-2023-5012	高危	升级至10.56及以上版本

在本年度总热度舆论榜前十的漏洞中，热度最高的漏洞为Nacos身份认证绕过漏洞(QVD-2023-6271)。该漏洞是由于开源服务管理平台Nacos在默认配置下未对 token.secret.key进行修改，导致远程攻击者可以绕过密钥认证进入后台，造成系统受控等后果。该系统通常部署在内网，用作服务发现及配置管理，历史上存在多个功能特性导致认证绕过、未授权等漏洞，建议升级至最新版本或修改默认密钥，并禁止公网访问，避免给业务带来安全风险。

02

安全漏洞大事件

第二章

本章节梳理了2023年度影响较大网络安全事件中关联的高危漏洞，这些漏洞已经被威胁行为体用于发起网络攻击，部分漏洞利用代码已在互联网上被公开，威胁程度极高，需要重点关注、优先修补。基于威胁情报的漏洞处理优先级排序对于威胁的消除能够起到事半功倍的效果。

一、 CVE-2023-7024 0day漏洞威胁数百万Chrome浏览器用户安全

事件描述

谷歌威胁分析小组安全研究团队的成员Vlad Stolyarov和Clément Lecigne发现了今年影响Chrome浏览器用户的第八个零日漏洞。Google威胁分析小组（Threat Analysis Group，TAG）在2023年12月19日报告，当时已发现针对该漏洞的攻击样本。

为了响应该漏洞，Google向所有Chrome用户发布了紧急修复补丁，CVE-2023-7024被评为高严重性漏洞，影响Chrome Web浏览器的开源WebRTC组件，属于堆缓冲区溢出类型。该实时通信组件支持网页内的音频和视频通信，并由大多数现代浏览器部署，任何基于Chromium项目的Web浏览器都易受到相同的攻击。谷歌提醒Windows用户，将Chrome版本升级到20.0.6099.129或20.0.6099.130；Linux和macOS用户升级到120.0.6099.129修复版本。

关联漏洞

1.1 Google Chrome WebRTC 堆缓冲区溢出漏洞(CVE-2023-7024)

WebRTC(Web Real-Time Communication)是一个由Google发起的实时通信开源项目，通过应用程序编程接口(API)为Web浏览器和移动应用程序提供实时通信(RTC)。它允许直接点对点通信，从而允许音频和视频通信在网页内进行，无需安装插件或下载本地应用程序。

奇安信CERT监测到Google修复Google Chrome WebRTC堆缓冲区溢出漏洞(CVE-2023-7024)，该漏洞存在在野利用，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或导致浏览器崩溃。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

修复建议

受影响版本	Google Chrome（Windows）版本：＜120.0.6099.129/130 Google Chrome（Mac/Linux）版本：＜120.0.6099.129
补丁链接	https://www.google.cn/chrome/
缓解措施	手动检查更新： 可通过Chrome 菜单-【帮助】-【关于 Google Chrome】检查版本更新， 并在更新完成后重新启动。

二、Citrix Bleed在有限的攻击中被作为零日漏洞滥用

事件描述

Mandiant表示，自2023年8月下旬以来，攻击者一直在利用CVE-2023-4966作为零日漏洞来窃取身份验证会话和劫持帐户。攻击者可以利用该漏洞绕过因素身份验证或其他强身份验证要求。即使在修补后，受感染的会话仍然存在，并且根据受感染账户的权限，攻击者可以在网络上横向移动或危及其他账户。此外，Mandiant还发现了利用CVE-2023-4966渗透政府实体和技术公司基础设施的案例。

CVE-2023-4966 Citrix Bleed缺陷是一个未经身份验证的缓冲区相关漏洞，影响Citrix NetScaler ADC和 NetScaler Gateway、用于负载平衡、防火墙实施、流量管理、VPN 和用户身份验证的网络设备。漏洞于2023年10月10日被披露，Citrix发布了补丁来修复该漏洞。

关联漏洞

2.1 NetScaler ADC 和 NetScaler Gateway 敏感信息泄露漏洞 (CVE-2023-4966)

Citrix NetScaler Gateway（以前称为Citrix Gateway）和NetScaler ADC（以前称为Citrix ADC）都是Citrix公司的产品。Citrix NetScaler Gateway是一套安全的远程接入解决方案。该方案可为管理员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 Systems NetScaler ADC是一个应用程序交付和安全平台。

奇安信CERT监测到官方更新 NetScaler ADC 和 NetScaler Gateway 敏感信息泄露漏洞(CVE-2023-4966)公告。

由于在snprintf格式化HTTP响应时，使用返回的长度作为参数读取内存，并且未验证长度范围，导致攻击者可以发送恶意请求读取Citrix Gateway内存，远程未授权攻击者可通过越界读写利用此漏洞最终可能造成敏感信息泄露，利用此漏洞无需额外条件。

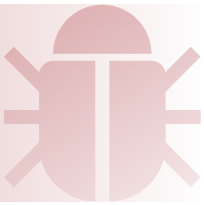
该漏洞已出现大规模野利用，目前官方已修复该漏洞，建议用户尽快升级至安全版本。

修复建议

受影响版本	NetScaler ADC and NetScaler Gateway 14.1 < 14.1-8.50 NetScaler ADC and NetScaler Gateway 13.1 < 13.1-49.15 NetScaler ADC and NetScaler Gateway 13.0 < 13.0-92.19 NetScaler ADC 13.1-FIPS < 13.1-37.164 NetScaler ADC 12.1-FIPS < 12.1-55.300 NetScaler ADC 12.1-NDcPP < 12.1-55.300

补丁链接	https://www.citrix.com/downloads/citrix-adc/ https://www.citrix.com/downloads/citrix-gateway/
缓解措施	升级 Citrix 系统到安全版本，需要注意的是，即使修复了漏洞，已被劫持的会话仍然可能有效，需要使用命令清除会话 clear lb persistentSession <vServer>

三、威胁行为体正在积极利用 F5 BIG-IP 远程代码执行漏洞



事件描述

2023年10月26日，F5向客户发出了一个严重安全漏洞CVE-2023-46747的公告，该漏洞CVSS评分9.8，影响BIG-IP，可能导致未经身份验证的远程代码执行。10月30日，F5更新最初的安全公告，称威胁行为体正在积极利用该漏洞。攻击者将该漏洞与BIG-IP配置实用程序中的另一个漏洞CVE-2023-46748结合使用。F5还发布了威胁指标(IoC)，以帮助防御者识别潜在威胁。

专家提醒，在漏洞PoC披露后不到五天，威胁行为体就开始利用F5 BIG-IP中的关键缺陷CVE-2023-46747。美国网络安全和基础设施安全局(CISA)将BIG-IP中的漏洞CVE-2023-46747和CVE-2023-46748添加到其已知被利用的漏洞目录中。

F5发布了针对易受攻击的F5 BIG-IP产品的修补程序。建议组织尽快修补易受攻击的F5 BIG-IP产品。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

关联漏洞

3.1 F5 BIG-IP 远程代码执行漏洞(CVE-2023-46747)

F5 BIG-IP 是美国 F5 公司一款集成流量管理、DNS、出入站规则、Web应用防火墙、Web网关、负载均衡等功能的应用交付平台。

奇安信CERT监测到F5 BIG-IP 远程代码执行漏洞(CVE-2023-46747)，未授权的远程攻击者可在暴露流量管理用户界面（TMUI）的 F5 BIG-IP 实例上执行任意代码。

修复建议

受影响版本	BIG-IP 17.x <= 17.1.0 16.1.0 <= BIG-IP <= 16.1.4 15.1.0 <= BIG-IP <= 15.1.10 14.1.0 <= BIG-IP <= 14.1.5 13.1.0 <= BIG-IP <= 13.1.5

补丁链接	https://my.f5.com/manage/s/downloads
缓解措施	1.阻止配置实用程序访问。 2.F5 BIG-IP 的易受攻击组件是配置实用程序。 对配置实用程序的访问应仅限于安全网络上受信任的用户和设备。 通过将每个自身 IP 地址的端口锁定设置更改为“不允许”，可以限制对配置实用程序的访问。 3.建议组织通过自身 IP 地址和管理界面阻止或限制对配置实用程序的访问。

关联漏洞

3.2 F5 BIG-IP SQL注入漏洞(CVE-2023-46748)

F5 BIG-IP 是美国 F5 公司一款集成流量管理、DNS、出入站规则、web应用防火墙、web网关、负载均衡等功能的应用交付平台。

F5 BIG-IP Configuration utility存在SQL注入漏洞，经过身份认证的远程攻击者利用该漏洞可以通过BIG-IP管理端口对配置实用程序进行网络访问，以执行任意系统命令。

修复建议

受影响版本	13.1.0<=BIG-IP<13.1.6 14.1.0<=BIG-IP<14.1.6 15.1.0<=BIG-IP<15.1.11 16.1.0<=BIG-IP<16.1.5 17.1.0<=BIG-IP<17.1.2
补丁链接	https://my.f5.com/manage/s/downloads
缓解措施	无

四、思科披露了新的IOS XE零日漏洞，可用于部署恶意软件植入

事件描述

2023年10月20日思科披露了一个新的高严重性零日漏洞（CVE-2023-20273），该漏洞被积极利用，在使用早些时候公布的CVE-2023-20198零日漏洞入侵的IOS XE设备上部署恶意植入程序。CVE-2023-20273用于获得root访问权限并完全控制Cisco IOS XE设备、部署恶意程序，使它们能够在系统上执行任意命令。

事件描述

根据Censys和LeakIX的估计，超过40,000台运行易受攻击的IOS XE软件的思科设备已经被黑客使用两个尚未修补的零日漏洞入侵。两天前，VulnCheck估计周二在10,000左右浮动，而Orange Cyberdefense CERT在一天后表示，它在34,500台IOS XE设备上发现了被植入恶意软件。

运行Cisco IOS XE的网络设备包括企业交换机、接入点、无线控制器以及工业路由器、聚合路由器和分支路由器。虽然很难获得暴露在互联网上的Cisco IOS XE设备的确切数量，但Shodan搜索目前显示，超过146000个易受攻击的系统受到攻击。

目前，思科已通过17.9.4a更新修复了17.9 Cisco IOS XE软件版本系列的这些漏洞，建议用户尽快更新。

关联漏洞

4.1 Cisco IOS XE Web UI 命令执行漏洞(CVE-2023-20273)

F5 BIG-IP 是美国 F5 公司一款集成流量管理、DNS、出入站规则、Web应用防火墙、Web网关、负载均衡等功能的应用交付平台。

奇安信CERT监测到F5 BIG-IP 远程代码执行漏洞(CVE-2023-46747)，未授权的远程攻击者可在暴露流量管理用户界面（TMUI）的 F5 BIG-IP 实例上执行任意代码。

修复建议

受影响版本	无
补丁链接	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z
缓解措施	如果启用HTTP Server或者HTTPS Server可以使用以下命令进行关闭： no ip http server/no ip http secure-server

关联漏洞

4.2 Cisco IOS XE 软件 Web UI 权限提升漏洞(CVE-2023-20198)

Web UI是一种基于GUI的嵌入式系统管理工具，能够提供系统配置、简化系统部署和可管理性以及增强用户体验。它带有默认映像，因此无需在系统上启用任何内容或安装任何许可证。Web UI 可用于构建配置以及监控系统和排除系统故障，而无需 CLI 专业知识。

Cisco IOS XE的Web UI存在权限提升漏洞，当Cisco IOS XE 软件的web UI暴露于互联网或不受信任的网络时，未经身份验证的远程攻击者可以利用该漏洞在受影响的系统上创建具有15级访问权限的账户。然后，攻击者可以使用该账户来控制受影响的系统。鉴于该产品用量较多且存在在野利用，建议客户尽快做好自查及防护。

修复建议

受影响版本	启用了HTTP或HTTP服务功能的Cisco IOS XE
补丁链接	https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html
缓解措施	禁用 HTTP/HTTPS 服务器功能或将这些功能部署于受信任网络。 可以使用no ip http server 或 no ip http secure-server 关闭HTTP/HTTPS 服务器功能。

五、用于传递基于Nim恶意软件诱骗Microsoft Word文档的武器化零日漏洞

关联漏洞

5.1 Windows SmartScreen安全特性绕过漏洞(CVE-2023-36025)

奇安信CERT监测到Windows SmartScreen上存在安全功能绕过漏洞，通过该漏洞能够绕过Windows Defender SmartScreen检查及其相关提示。未经身份认证的远程攻击者可以诱骗受害者单击特制的.URL文件并在系统上执行任意代码。该漏洞存在在野利用。

修复建议

受影响版本	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 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 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 Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows Server 2012 R2 (Server Core installation)

修复建议

受影响版本	Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows 11 Version 23H2 for ARM64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based 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 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 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
补丁链接	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025
缓解措施	目前微软已发布安全更新，用户可通过 Windows 更新获取，若无法自动更新，可参考链接下载并安装相应版本的安全补丁

六、Apple修复了用于秘密传送间谍软件的零日漏洞

事件描述

2023年3月27日，苹果公司发布在野外被利用的零日漏洞CVE-2023-32435的补丁。

卡巴斯基安全研究人员透露，他们的一些公司iOS设备上安装了以前未知的间谍软件。感染是通过iMessage发生的——受害者收到一条带有附件的消息，其中包含一个漏洞，该漏洞会触发一个允许执行代码的漏洞，利用未知硬件接口绕过保护措施，对任意内核地址进行读写，从C2服务器下载其他恶意软件。最后，删除附件中的初始消息和漏洞。受害者不需要打开iMessage就可以发生感染。

关联漏洞

6.1 Apple iPadOS WebKit 代码执行漏洞(CVE-2023-32435)

Apple macOS Ventura是美国Apple公司的一个桌面操作系统。

奇安信CERT监测到Apple官方发布了多个产品高危漏洞，包括Apple iPadOS WebKit代码执行漏洞(CVE-2023-32435)。iOS 和 iPadOS 中存在代码执行漏洞，DEL未经身份认证的远程攻击者诱导受害者打开特制的网站后触发该漏洞，成功利用该漏洞可以执行代码。

目前，该漏洞已发现在野利用，建议客户尽快修复，以防止潜在的利用。

修复建议

受影响版本	safari < 16.4 iOS < 16.4	macOS Ventura < 13.3 iOS < 15.7.7	PadOS < 16.4 iPadOS < 15.7.7
补丁链接	https://support.apple.com/en-us/HT213670 https://support.apple.com/en-us/HT213671 https://support.apple.com/en-us/HT213676 https://support.apple.com/en-us/HT213811		
缓解措施	无		

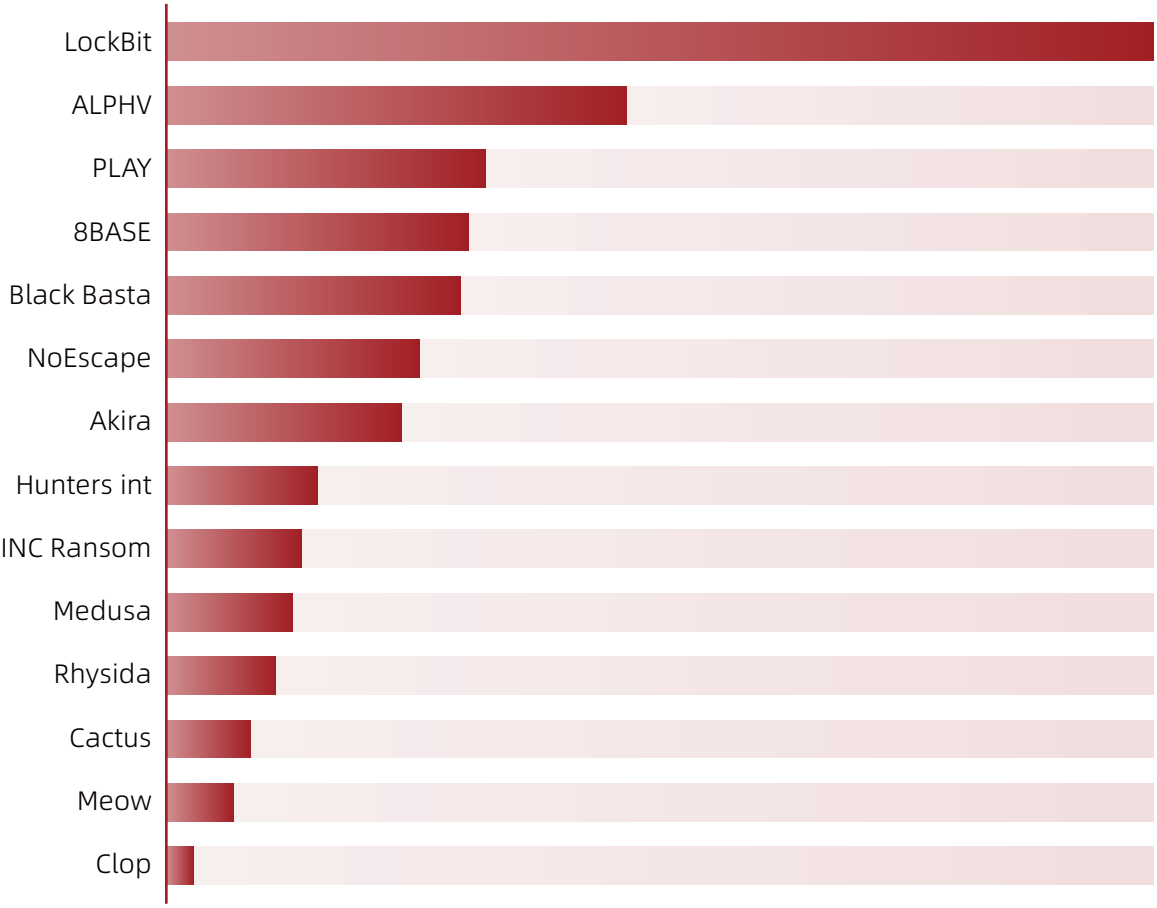
03

勒索软件攻击中使用的漏洞

第三章

2023年勒索攻击事件频发，勒索软件团伙活跃度排名如图3-1所示。了解勒索软件攻击中利用的主要漏洞对企业安全防护能力建设至关重要。通过优先考虑漏洞缓解、及时应用补丁并遵循网络安全准则，可以降低成为勒索软件攻击受害者的风险。

2023年勒索软件团伙活跃度排名



△图3-1 2023年流行勒索软件排名

2023年流行勒索软件关联漏洞如图3-2所示。本节全面总结了2023年勒索软件攻击中利用的关键漏洞，强调主动预防和有效事件响应的必要性。

LOCKBIT 3.0	LockBit	Citrix Netscaler ADC & Gateway信息泄露漏洞(CVE-2023-4966)
	Cactus	Atlassian Confluence 身份认证绕过漏洞(CVE-2023-22518) Qlik Sense 路径遍历漏洞(CVE-2023-41266) Qlik Sense HTTP请求隧道漏洞(CVE-2023-41265) Qlik Sense 远程代码执行漏洞(CVE-2023-48365)
	clop	Progress MOVEit Transfer sQL注入漏洞(CVE-2023-34362) GoAnywhere MFT命令执行漏洞(CVE-2023-0669)
	Akira	Cisco 多个产品安全特性绕过漏洞(CVE-2023-20269)

△图3-2 2023年流行勒索软件关联漏洞

一、 LockBit勒索软件使用的Citrix Bleed漏洞

事件描述

Lockbit 勒索软件利用CVE-2023-4966来破坏大型组织的系统、窃取数据和加密文件，该漏洞是一个是一个严重程度极高、可远程利用的信息泄露漏洞。

2023年10月10日，Citrix发布了有关影响NetScaler ADC和NetScaler Gateway设备的敏感信息泄露漏洞(CVE-2023-4966)的安全公告，声称已修复漏洞，但成千上万个暴露在互联网上的端点仍在运行易受攻击的设备。

2023年11月10日，中国工商银行（ICBC）的美国全资子公司工银金融服务有限责任公司（ICBCFS）在官网发布申明称11月8日遭受了LockBit勒索软件攻击，导致部分系统中断。

攻击发生后，由于被攻击的系统被隔离断网，工行总部和其他海外分支机构并未受到影响，但也导致工银金融无法清算待处理的美国国债交易，被迫通过U盘发送结算数据。据报道，对工商银行美国子公司的攻击已经扰乱了美国国债市场。

安全专家推测，攻击者可能利用了未及时修补的Citrix Bleed漏洞（CVE-2023-4966）。

关联漏洞

1.1 NetScaler ADC 和 NetScaler Gateway 敏感信息泄露漏洞 (CVE-2023-4966)

Citrix NetScaler Gateway（以前称为Citrix Gateway）和NetScaler ADC（以前称为Citrix ADC）都是Citrix公司的产品。Citrix NetScaler Gateway是一套安全的远程接入解决方案。该方案可为管理员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 Systems NetScaler ADC是一个应用程序交付和安全平台。

奇安信CERT监测到官方更新NetScaler ADC 和 NetScaler Gateway敏感信息泄露漏洞(CVE-2023-4966)公告，由于在snprintf格式化HTTP响应时，使用返回的长度作为参数读取内存，并且未验证长度范围，导致攻击者可以发送恶意请求读取Citrix Gateway内存，远程未授权攻击者可通过越界读写利用此漏洞最终可能造成敏感信息泄露，利用此漏洞无需额外条件。

该漏洞已出现大规模在野利用，目前官方已修复该漏洞，建议用户尽快升级至安全版本。

修复建议

受影响版本	NetScaler ADC and NetScaler Gateway 14.1 < 14.1-8.50 NetScaler ADC and NetScaler Gateway 13.1 < 13.1-49.15 NetScaler ADC and NetScaler Gateway 13.0 < 13.0-92.19 NetScaler ADC 13.1-FIPS < 13.1-37.164 NetScaler ADC 12.1-FIPS < 12.1-55.300 NetScaler ADC 12.1-NDcPP < 12.1-55.300
补丁链接	https://www.citrix.com/downloads/citrix-adc/ https://www.citrix.com/downloads/citrix-gateway/
缓解措施	1.升级Citrix系统到安全版本； 2.需要注意的是，即使修复了漏洞，已被劫持的会话仍然可能有效，需要使用命令清除会话：clear lb persistentSession <vServer>

二、Akira勒索的组织使用的Cisco产品漏洞

事件描述

勒索软件Akira利用思科SSL VPN漏洞CVE-2023-20269入侵组织内部网络环境，加密Windows、Linux电脑档案。该漏洞存在于Cisco的网络自适应安全设备ASA、FTD系列，攻击者可在未经授权的情况下，借由暴力破解攻击找出有效的帐号及密码，甚至有可能透过未经授权的用户，建立无客户端的SSL VPN连线。2023年8月勒索软件Akira攻击态势持续延烧，成为排名前10大的勒索软件家族，超过110个组织遭Akira锁定。

关联漏洞

2.1 Cisco 多个产品安全特性绕过漏洞(CVE-2023-20269)

思科自适应安全设备（ASA）软件和思科Firepower Threat Defense（FTD）软件中的远程访问VPN功能存在漏洞，可能允许未经身份验证的远程攻击者通过暴力破解攻击来尝试识别有效的用户名和密码组合，或者允许经过身份验证的远程攻击者与未经授权的用户建立无客户端SSL VPN会话。

修复建议

受影响版本	Cisco FTD Software 7.0.6 Cisco FTD Software 7.2.5
补丁链接	https://software.cisco.com/download/home

缓解措施	无

三、勒索软件团伙使用的0day漏洞

事件描述

以Clop勒索软件为首的多个团伙，在本年度利用多个最新0day漏洞发起勒索软件攻击，例如 MOVEit Transfer、PaperCut、GoAnywhere MFT等。

2023年5月下旬，几乎数百家企业的云数据库同时遭到非法访问，黑客利用MOVEit的0day漏洞CVE-2023-34362，获得了企业网络存储库的完全访问权限，这意味着他们可以窃取所有文件，尽管厂商及时发布了漏洞补丁，但已为时已晚。MOVEit漏洞至少影响2500家企业，损失或超百亿。

PaperCut漏洞是PaperCut NG/MF打印管理软件中的一个严重远程代码执行漏洞。CVE-2023-27350和CVE-2023-27351两个0day漏洞于2023年3月首次披露，已被Clop、LockBit和Bl00dy等勒索软件攻击者利用。CVE-2023-27350漏洞允许攻击者无需身份验证即可在易受攻击的系统上执行任意代码。这可用于安装勒索软件、窃取数据或中断操作。允许未经身份验证的攻击者在PaperCut应用程序服务器上远程执行代码。CVE-2023-27351允许未经身份验证的攻击者获取PaperCut NG/MFs中存储的有关用户的信息。

根据报告，3 月份勒索软件攻击创下新高的原因是Fortra的GoAnywhere MFT 安全文件传输工具中的一个0day漏洞CVE-2023-0669利用。勒索软件组织Clop利用该漏洞在十天内从130家公司窃取了数据。

关联漏洞

3.1 Progress MOVEit Transfer SQL注入漏洞(CVE-2023-34362)

在MOVEit Transfer Web应用程序中存在SQL注入漏洞，该漏洞允许远程未经授权的攻击者获得对MOVEit Transfer数据库的访问权限，并根据所使用的数据库引擎（MySQL、Microsoft SQL Server 或 Azure SQL），除了执行更改或删除数据库元素的SQL语句外，还可能推断出有关数据库结构和内容的信息，造成敏感信息泄露，进一步利用可能获取服务器权限。目前该漏洞已出现在野利用，建议受影响用户尽快修复。

修复建议

受影响版本	2021.0.0 < MOVEit Transfer < 2021.0.6 (13.0.6) 2021.1.0 < MOVEit Transfer < 2021.1.4 (13.1.4) 2022.0.0 < MOVEit Transfer < 2022.0.4 (14.0.4) 2022.1.0 < MOVEit Transfer < 2022.1.5 (14.1.5) 2023.0.0 < MOVEit Transfer < 2023.0.1 (15.0.1)
补丁链接	https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023 https://docs.ipswitch.com/MOVEit/Transfer2020_1/ReleaseNotes/en/
缓解措施	限制所有流向MOVEit Transfer的HTTP和HTTPs流量

关联漏洞

3.2 PaperCut NG和MF 身份认证绕过漏洞(CVE-2023-27350)

PaperCut NG/MF打印管理软件存在身份认证绕过漏洞，此漏洞允许远程攻击者绕过受影响的Paper-Cut NG安装的身份验证，不需要身份验证。由于访问控制不当造成的，导致SetupCompleted类中存在缺陷，攻击者可以利用此漏洞绕过身份验证并在SYSTEM上下文中执行任意代码。

修复建议

受影响版本	PaperCut NG >= 8.0 PaperCut MF >= 8.0
补丁链接	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219#faqs
缓解措施	1.对PaperCut服务器的远程访问：可以通过将服务器的侦听端口从 8080 更改为非标准端口来完成。 2.PaperCut账户使用强密码和多重身份验证：有助于防止攻击者未经授权访问有风险的服务器。 3.视PaperCut服务器是否存在可疑活动：可以通过使用安全信息和事件管理(SIEM)工具或手动查看日志文件来完成。

关联漏洞

3.3 PaperCut MF/NG 信息泄露漏洞(CVE-2023-27351)

PaperCut NG/MF打印管理软件存在信息泄露漏洞，未经身份验证的攻击者可利用该漏洞提取存储在Papercut MF/NG中的用户信息，包括用户名、电子邮件地址、办公室/部门信息以及与用户关联的任何卡号。DEL攻击者还可以利用该漏洞提取密码哈希值。

修复建议

受影响版本	15.0.0 <= PaperCut MF/NG <= 19.2.7 20.0.0 <= PaperCut MF/NG <= 20.1.6 21.0.0 <= PaperCut MF/NG <= 21.2.10 22.0.0 <= PaperCut MF/NG <= 22.0.8
补丁链接	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219#faqs
缓解措施	1.用对PaperCut服务器的远程访问：可以通过将服务器的侦听端口从8080 更改为非标准端口来完成。 2.PaperCut账户使用强密码和多重身份验证：有助于防止攻击者未经授权访问有风险的服务器。 3.视PaperCut服务器是否存在可疑活动：可以通过使用安全信息和事件管理(SIEM)工具或手动查看日志文件来完成。

关联漏洞

3.4 GoAnywhere MFT命令执行漏洞(CVE-2023-0669)

HelpSystems GoAnywhere MFT是美国HelpSystems公司的一款托管文件传输软件。GoAnywhere MFT 中存在反序列化漏洞，远程攻击者可通过发送特制的序列化对象至管理端口，服务端接收此请求未进行过滤从而反序列化任意攻击者控制的对象，最终导致任意代码执行。

修复建议

受影响版本	GoAnywhere MFT < 7.1.2
补丁链接	https://www.goanywhere.com/
缓解措施	限制管理端口网络访问

四、 Qlik Sense 应用程序漏洞

事件描述

研究人员观察到Qlik Sense在Cactus勒索软件活动中被利用，该活动利用了Qlik Sense应用程序中的多个漏洞。目前评估认为，根据补丁级别，威胁行为体很可能通过组合或直接利用Qlik Sense中的CVE-2023-41266、CVE-2023-41265或潜在的CVE-2023-48365来实现代码执行。这是部署Cactu勒索软件的威胁行为体首次利用Qlik Sense中的漏洞进行初始访问。

关联漏洞

4.1 Qlik Sense 路径遍历漏洞(CVE-2023-41266)

Qlik Sense 是一个现代分析平台，旨在帮助用户创建具有数据素养的员工队伍并实现业务转型。

Qlik Sense Enterprise for Windows存在目录遍历漏洞。由于对用户提供的输入的验证不正确，未经身份验证的远程攻击者可能会生成匿名会话，从而允许他们向未经授权的端点执行 HTTP 请求。该漏洞结合CVE-2023-41265一起利用，可以实现未授权RCE。

修复建议

受影响版本	Qlik Sense Enterprise for Windows <= May 2023 Patch 3 Qlik Sense Enterprise for Windows <= February 2023 Patch 7 Qlik Sense Enterprise for Windows <= November 2022 Patch 10 Qlik Sense Enterprise for Windows <= August 2022 Patch 12
补丁链接	https://github.com/qlik-download/qlik-sense-desktop/releases/tag/v14.159.5
缓解措施	限制所有流向MOVEit Transfer的HTTP和HTTPs流量

关联漏洞

4.2 Qlik Sense HTTP请求隧道漏洞(CVE-2023-41265)

Qlik Sense Enterprise for Windows存在请求隧道漏洞，由于HTTP请求头验证不当，远程攻击者能够通过隧道传输HTTP请求来提升其权限，从而允许他们在托管存储库应用程序的后端服务器上执行HTTP请求。

修复建议

受影响版本	Qlik Sense Enterprise for Windows <= May 2023 Patch 3 Qlik Sense Enterprise for Windows <= February 2023 Patch 7 Qlik Sense Enterprise for Windows <= November 2022 Patch 10 Qlik Sense Enterprise for Windows <= August 2022 Patch 12
补丁链接	https://github.com/qlik-download/qlik-sense-desktop/releases/tag/v14.159.5
缓解措施	无

关联漏洞

4.3 Qlik Sense 远程代码执行漏洞(CVE-2023-48365)

Qlik Sense Enterprise for Windows存在代码执行漏洞，该漏洞由于对HTTP标头的验证不正确，远程攻击者能够通过隧道传输HTTP请求来提升权限，从而允许攻击者在托管存储库应用程序的后端服务器上执行HTTP请求，导致远程代码执行。

修复建议

受影响版本	Qlik Sense Enterprise for Windows <= Augu st 2023 Patch 1 Qlik Sense Enterprise for Windows <= May 2023 Patch 5 Qlik Sense Enterprise for Windows <= February 2023 Patch 9 Qlik Sense Enterprise for Windows <= November 2022 Patch 11 Qlik Sense Enterprise for Windows <= August 2022 Patch 13 Qlik Sense Enterprise for Windows <= May 2022 Patch 15 Qlik Sense Enterprise for Windows <= February 2022 Patch 14 Qlik Sense Enterprise for Windows <= November 2021 Patch 16
补丁链接	https://github.com/qlik-download/qlik-sense-desktop/releases/tag/v14.159.5
缓解措施	无

五、IBM Aspera Faspex 文件共享软件漏洞

事件描述

IBM Aspera Faspex文件共享软件漏洞CVE-2022-47986是一个严重的远程执行代码漏洞，影响IBM Aspera Faspex .4.2及更早版本。该漏洞于2023年1月披露，已被包括IceFire勒索软件组织在内的勒索软件攻击者利用。

关联漏洞

5.1 IBM Aspera Faspex 代码执行漏洞(CVE-2022-47986)

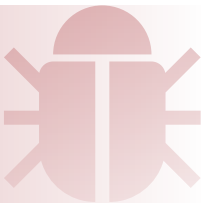
IBM Aspera Faspex是一种快速的全球个人对个人文件交付和协作解决方案。用户可以使用标准的网络浏览器、桌面应用程序或移动应用程序，以电子邮件样式的工作流程在地理分散的团队之间高速发送和接收无限大小的数字包。

IBM Aspera Faspex是一种快速的全球个人对个人文件交付和协作解决方案。用户可以使用标准的网络浏览器、桌面应用程序或移动应用程序，以电子邮件样式的工作流程在地理分散的团队之间高速发送和接收无限大小的数字包。

修复建议

受影响版本	IBM Aspera Faspex <= 4.4.2 Patch Level 1
补丁链接	https://www.ibm.com/docs/fr/aspera-faspex/5.0?topic=welcome-faspex
缓解措施	无

六、各类权限提升漏洞



事件描述

勒索软件威胁团体经常利用各种权限升级漏洞作为其攻击的一部分。CVE-2022-24521就是此类漏洞之一，它影响Windows通用日志文件系统。该漏洞已于2022年4月修复，攻击者成功利用该漏洞后即可提升权限。已知古巴、RedAlert和Yanluowang等著名勒索软件组织在攻击中利用CVE-2022-24521。

另一个被用于提权的漏洞称为PrintNightmare，漏洞编号为CVE-2021-34527。该漏洞已于2021年7月修复，但已被BlackBasta组织的附属公司利用。通过利用此漏洞，他们能够在获得网络的初始访问权限后执行特权操作。

此外，Nokoyawa勒索软件组织已被发现利用漏洞CVE-2023-28252。该漏洞影响Windows通用日志文件系统，已于2023年4月修复。与CVE-2022-24521类似，该漏洞允许攻击者在受感染系统中提升权限。

关联漏洞

6.1 Windows 通用日志文件系统权限提升漏洞(CVE-2022-24521)

Windows 通用日志文件系统存在权限提升漏洞，该漏洞允许本地用户提升权限。由于Windows common log file system driver程序中的边界错误，本地非特权用户可以运行一个特制的程序来触发内存损坏并执行任意代码，提升权限，需要注意的是，这个漏洞已发现在野利用。2023年4月补丁日，微软修复了CLFS中的一个类似的在野利用漏洞CVE-2022-24521。

修复建议

受影响版本	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 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
补丁链接	https://catalog.update.microsoft.com/Search.aspx?q=KB5012599
缓解措施	无

关联漏洞

6.2 Windows Print Spooler远程代码执行漏洞(CVE-2021-34527)

Windows的Windows Print Spooler中存在远程代码执行漏洞，该服务错误的执行特权文件操作时导致了该漏洞的产生，成功利用此漏洞的攻击者可以使用系统权限运行任意代码。

修复建议

受影响版本	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 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
补丁链接	https://catalog.update.microsoft.com/Search.aspx?q=KB5004958

缓解措施	一、禁用打印服务： 确定服务是否在运行（使用powershell） Get-Service -Name spooller 如果该服务在运行则使用以下命令停止该服务（使用poeweshell） Stop-Service -Name Spooler -Force Set-Servicwe -Name Spooler -StartupType Disabled

关联漏洞

6.3 Windows 通用日志文件系统权限提升漏洞(CVE-2023-28252)

Windows通用日志文件系统驱动程序存在权限提升漏洞，本地攻击者可以利用该漏洞创建恶意日志文件触发漏洞，攻击者可以利用该漏洞将自身权限提升至SYSTEM权限，目前该漏洞已发现在野利用事件。

修复建议

受影响版本	Windows 11 Version 22H2 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows Server 2016 (Server Core installation) Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2012 R2 (Server Core installation)
补丁链接	https://catalog.update.microsoft.com/Search.aspx?q=KB5025288
缓解措施	无

04

关键漏洞回顾

第四章

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标记为“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。

2023年共标记关键漏洞824个，占全年新增漏洞的2.76%。其中有公开Exploit/PoC漏洞数量为631个，占全年新增漏洞的2.12%；发现在野利用漏洞数量为264个，占全年新增漏洞的0.88%；0day漏洞数量为75个，占全年新增漏洞的0.25%；APT相关漏洞数量为18个，占全年新增漏洞的0.06%。各类关键漏洞在2023年新增漏洞中占比情况如图4-1所示：

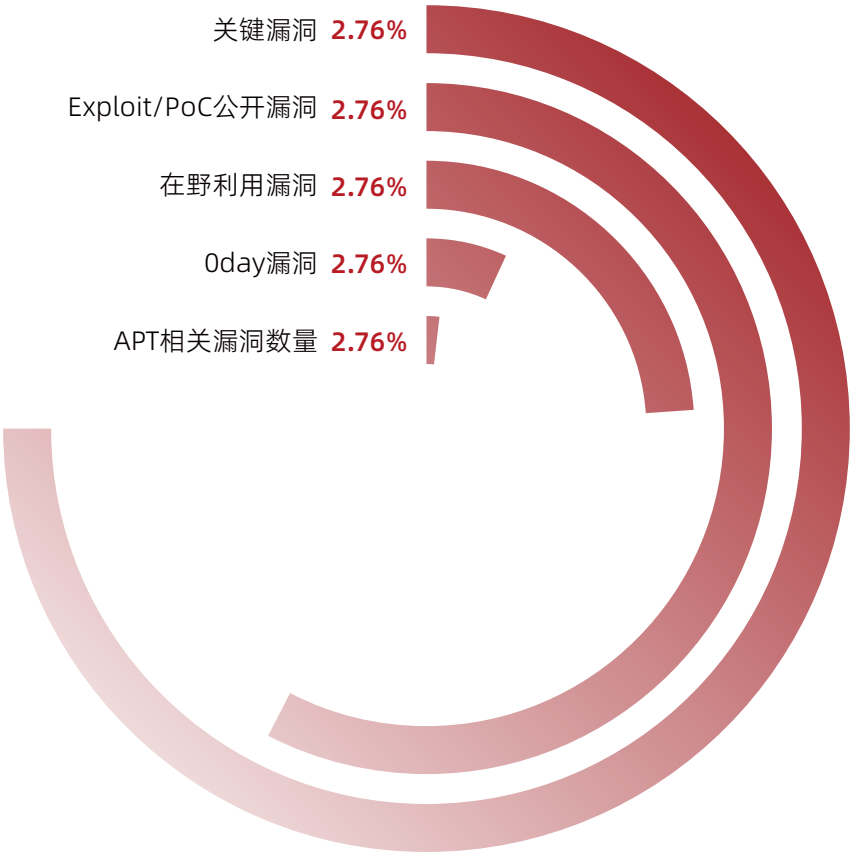
824个
2023年共标记关键漏洞
占全年新增漏洞的2.76%

631个
公开Exploit/PoC漏洞
占全年新增漏洞的2.12%

264个
在野利用漏洞
占全年新增漏洞的0.88%

75个
0day漏洞
占全年新增漏洞的0.25%

18个
APT相关漏洞
占全年新增漏洞的0.06%



△图4-1 各类关键漏洞在全年新增漏洞中占比情况

一、0day漏洞回顾

2023年新增的0day漏洞中有92%的漏洞发现在野利用，有42.7%的漏洞发现公开Exploit/PoC。近一半发现在野利用的0day漏洞没有没有监测到公开的利用代码，处于私有状态，仅被某些APT组织或者个人使用。本章节回顾了2023年部分影响较大的0day漏洞。

1.1 Cisco IOS XE 软件 Web UI权限提升漏洞(CVE-2023-20198)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-20198	权限提升	10	是	已公开	已公开	已发现

Cisco IOS XE 是思科（Cisco）公司的一个操作系统，用于驱动其网络设备和路由器。它是一个在Cisco设备上运行的网络操作系统，旨在提供高性能、可扩展性和安全性，以满足不同规模和类型的网络需求。

2023年10月17日思科发布通告称Cisco IOS XE软件Web UI权限提升漏洞(CVE-2023-20198)与Cisco IOS XE Web UI命令执行漏洞(CVE-2023-20273)存在在野利用。这些漏洞影响所有启用了Web UI功能的Cisco IOS XE设备，利用CVE-2023-20198允许未经认证的远程攻击者在受影响的系统上创建一个权限级别为15的账户，攻击者可以完全访问所有命令，包括重载系统和更改配置的命令。攻击者可以使用该账户获得对受影响系统的控制权。随后利用CVE-2023-20273发送特制的请求以root权限执行任意命令。经过威胁行为体的精心策划与实施，这些漏洞已被广泛利用，奇安信威胁情报中心于10月25日观察到全球有两万五千余台设备被植入后门。

1.2 WPS Office 代码执行漏洞(QVD-2023-17241)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
QVD-2023-17241	代码执行	8.6	是	已公开	已公开	已发现
QVD-2023-19351	代码执行	8.6	是	已公开	已公开	已发现

WPS Office 是金山办公软件出品的 office 软件，可以实现办公软件常用的文字、表格、演示等多种功能。

2023年7月27日，奇安信红雨滴高级威胁研究团队捕获WPS Office 代码执行漏洞(QVD-2023-17241)在野利用样本，随后报送此漏洞到WPS office官方，官方于8月9日披露并修复此漏洞。攻击者通过诱导用户打开文档中嵌入的远程链接即可触发此漏洞执行任意代码。8月22日红雨滴团队再次捕获WPS Office代码执行漏洞(QVD-2023-19351)在野利用样本，官方于8月23日修复此漏洞。这些漏洞都是因为在docx文档中插入了浏览器对象WebShape，由于WPS使用Chrome嵌入式框架（CEF），该对象可以直接调用Chrome渲染Html网页，从而执行恶意代码。

1.3 Microsoft Outlook 权限提升漏洞(CVE-2023-23397)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-23397	权限提升	9.8	是	已公开	已公开	已发现

Microsoft Outlook是由微软公司开发的个人信息管理系统软件，功能包括收发电子邮件、日历等。outlook主要用来发送电子邮件，同时包含了日历、任务管理、联系人、记事本等功能。

在2023年3月14日，微软发布了在野0day Microsoft Outlook权限提升漏洞（CVE-2023-23397）。该漏洞由乌克兰计算机应急小组向微软报告，微软将这次攻击归咎于俄罗斯黑客。研究人员观察到了来自俄罗斯的组织Forest Blizzard涉及修改Microsoft Exchange服务器内邮箱文件夹权限的技术。它允许攻击者提供对电子邮件通信的秘密、未经授权的访问，并在通过CVE-2023-23397或密码喷射获得对电子邮件帐户的访问权限后使用。

1.4 Microsoft 流式处理代理权限提升漏洞(CVE-2023-36802)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-36802	权限提升	7.8	是	已公开	已公开	已发现

Windows内核是Windows操作系统的核心组件，它是操作系统的底层部分，负责管理和协调计算机硬件和软件资源。内核提供了操作系统的基本功能和服务，包括进程管理、内存管理、设备驱动程序、文件系统、网络通信等。

2023年9月12日微软补丁日修复此在野漏洞，10月11日此漏洞技术细节与EXP在互联网上公开。由于Windows多媒体框架服务中的组件Microsoft Kernel Streaming Server (mskssrv.sys)中存在对象类型混淆漏洞，具有低权限的本地攻击者通过该漏洞可以在越界内存上执行流对象操作，从而在内核中执行恶意代码，最终可以将权限提升至SYSTEM。该模块还有一个6月修复的“品相极好”的逻辑漏洞CVE-2023-29360，同一个模块中有完整的漏洞利用链，不需要破坏对象也不需要内存布局便可利用。

1.5 Windows 通用日志文件系统驱动程序权限提升漏洞 (CVE-2023-28252)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-28252	权限提升	7.8	是	已公开	已公开	已发现

CLFS(Common Log File System)是Windows中的一种日志文件系统,主要用于存储需要高性能写入的日志文件。CLFS常用于需要高效写入大量日志的数据的应用场景中,如数据库日志、事件跟踪日志等。相比普通NTFS文件系统,CLFS可以提供更高的日志写入吞吐量和更低的写入延迟。

该漏洞是由于内核的clfs驱动会尝试从BLF文件中读取control record的iFlushBlock并使用该值作为偏移定位rgContainers，然而clfs驱动获取到iFlushBlock之后并没有验证其是否是有效的，导致攻击者可以修改iFlushBlock，使得clfs驱动定位到错误rgContainers，之后的越界读取攻击者控制的内存，并执行攻击者伪造的对象的函数指针，从而在内核执行任意代码。Clfs驱动由于历史悠久，近几年来一直是热门的漏洞挖掘对象，在2022年同样有在野利用的漏洞CVE-2022-37969 Windows CLFS权限提升漏洞。

二、APT相关漏洞回顾

2023年APT关联漏洞如图4-2所示。本节回顾了2023年部分影响较大的APT事件相关漏洞，完整APT活动相关漏洞列表见附录1。

	未知 （高度疑似NSA）	Apple 特殊字体代码执行漏洞(CVE-2023-41990) Apple Kernel 权限提升漏洞(CVE-2023-32434) Apple WebKit 代码执行漏洞(CVE-2023-32435) Apple iPhone硬件安全机制Page Protection Layer 绕过漏洞(CVE-2023-38606)
	Lazarus	Apache ActiveMQ 远程代码执行漏洞(CVE-2023-46604) JetBrains TeamCity 身份认证绕过漏洞(CVE-2023-42793)
	APT28	RARLAB WinRAR 代码执行漏洞(CVE-2023-38831) Microsoft Outlook 权限提升漏洞(CVE-2023-23397)
	Storm-0978	Windows Search远程代码执行漏洞(CVE-2023-36584)
	Labyrinth Chollima	3CXDesktop App 代码执行漏洞(CVE-2023-29059)

△图4-2 2023年APT组织关联漏洞

2.1 Apple Operation Triangulation多个漏洞

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-41990	代码执行	8.3	是	未公开	未公开	已发现
CVE-2023-32434	权限提升	8	是	未公开	未公开	已发现
CVE-2023-38606	安全特性绕过	7.8	是	未公开	未公开	已发现

CVE-2023-32435	代码执行	8.8	是	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。Apple WebKit是由苹果开发的一款开源浏览器引擎，它是Safari浏览器的核心组件，也被Google、Adobe等公司使用在其产品中。

卡巴斯基自2023年6月1日曝光Operation Triangulation攻击行动后发布多篇报告，此行动涉及4个0-day漏洞的使用：Apple 特殊字体代码执行漏洞(CVE-2023-41990)、Apple Kernel权限提升漏洞(CVE-2023-32434)、Apple iPhone硬件安全机制Page Protection Layer绕过漏洞(CVE-2023-38606)、Apple WebKit代码执行漏洞(CVE-2023-32435)。卡巴斯基称其内部重要员工的iPhone手机从2019年开始就遭到0-day漏洞的攻击，此次行动的受害者可能涉及多个国家的重点公司及政府部门。奇安信威胁情报中心依赖奇安信内部相关数据，确认Operation Triangulation行动同样波及了国内多个重点单位的重要人员。

Operation Triangulation攻击链无需用户交互（0-click），并且适用的iOS版本可至16.2。攻击第一阶段通过iMessage发送带字体漏洞CVE-2023-41990的pdf文件，漏洞触发配合CVE-2023-32434/CVE-2023-38606实现完整的代码执行权限，之后清除了设备中的所有漏洞利用痕迹并转入第二阶段的Safari利用流程，中间会有一个受害者鉴定的操作，完成后通过Safari漏洞CVE-2023-32435配合CVE-2023-32434/CVE-2023-38606再次实现完整的代码执行权限，并投递恶意软件。

2.2 Apache ActiveMQ 远程代码执行漏洞(CVE-2023-46604)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-46604	代码执行	10	是	已公开	已公开	已发现

ActiveMQ是一个开源的消息代理和集成模式服务器，它支持Java消息服务(JMS) API。它是Apache Software Foundation下的一个项目，用于实现消息中间件，帮助不同的应用程序或系统之间进行通信。

2023年10月25日，Apache修复Apache ActiveMQ 远程代码执行漏洞(CVE-2023-46604)。该漏洞可能允许对broker具有网络访问权限的远程攻击者通过操纵OpenWire协议中的序列化类类型来实例化类路径上的任何类，最终可导致执行任意命令。在10月27日，Rapid7托管检测和响应(MDR)发现疑似Apache ActiveMQ 远程代码执行漏洞(CVE-2023-46604)利用的情况，HelloKitty勒索软件家族试图在受害者机器上布置勒索软件，攻击者成功利用后，会通过MSIExec加载远程二进制文件，再对本地文件进行加密，在11月，AhnLab安全应急响应中心（ASEC）在监控Andariel威胁组织近期的攻击时，发现了该组织利用Apache ActiveMQ远程代码执行漏洞（CVE-2023-46604）安装恶意软件的攻击案例。

2.3 JetBrains TeamCity 身份认证绕过漏洞(CVE-2023-42793)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-46604	身份认证绕过	10	是	已公开	已公开	已发现

TeamCity是一个通用CI/CD软件平台，可实现灵活的工作流程、协作和开发实践。2023年10月，微软发现2个朝鲜的APT组织Diamond Sleet和Onyx Sleet正在利用JetBrains TeamCity身份认证绕过漏洞(CVE-2023-42793)实施供应链攻击。同年12月美国联邦调查(FBI)、美国网络安全和基础设施安全局、美国国家安全局(NSA)、波兰军事反情报局(SKW)、波兰CERT(CERT.PL)和英国国家网络安全中心(NCSC)发现SVR组织正在大规模利用该漏洞实施APT攻击。

JetBrains TeamCity 存在身份认证绕过漏洞，未经身份验证的远程攻击者可以向tokens/RPC2接口发送恶意请求，即可绕过身份验证添加任意权限用户，进一步利用可在TeamCity服务器执行任意代码。攻击者可以利用该漏洞添加管理员账号，进入后台获取或修改软件开发人员的源代码、签署证书或进一步实施供应链攻击。

2.4 RARLAB WinRAR 代码执行漏洞(CVE-2023-38831)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-38831	代码执行	8.6	是	已公开	已公开	已发现

WinRAR是一款功能强大的压缩包管理器，它是档案工具RAR在Windows环境下的图形界面。该软件可用于备份数据，缩减电子邮件附件的大小，解压缩从 Internet上下载的RAR、ZIP及其它类型文件，并且可以新建RAR及ZIP格式等的压缩类文件。目前已监测到多个APT组织利用该漏洞。

在2023年7月国外安全厂商监测到早在2023年4月就有黑客利用该漏洞攻击交易员，尝试盗取其账户上的资金，该漏洞是由于winrar尝试打开压缩包内的文件时，如果文件名后面带有空格则WinRAR会错误的释放同名目录下的文件到临时目录，而后尝试，使用ShellExecuteExW打开该文件，而ShellExecuteExW会在路径末尾添加.*通配符并搜索，从而导致ShellExecuteExW打开了之前释放的恶意文件，在目标系统上执行任意代码。随后在2023年9月CERT-UA发布了有关俄罗斯GRU组织FROZENLAKE（又名APT28）使用该漏洞制作钓鱼文档的信息，该APT组织利用该漏洞进行鱼叉式钓鱼，尝试在目标系统上执行Power-Shell。

2.5 Windows Search远程代码执行漏洞(CVE-2023-36584)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-36884	代码执行	8.0	是	已公开	未公开	已发现

Windows Search是Windows操作系统中的一个功能，旨在提供快速和便捷的文件和应用程序搜索功能。

2023年7月4日黑莓威胁研究和情报团队发现Storm-0978利用此漏洞攻击北约峰会相关参会人员。7月11日微软发布此漏洞缓解方案，最终于8月8日补丁日发布此漏洞补丁。未经身份验证的远程攻击者向受害者发送文档文件，一旦受害者打开文件，便会触发漏洞执行恶意代码。Storm-0978还使用了Windows Mark of the Web安全功能绕过漏洞(CVE-2023-36584)、Windows SmartScreen安全功能绕过漏洞(CVE-2023-36025)构成攻击链。TA544组织也曾利用CVE-2023-36025。安全研究员在对Storm-0978的样本分析中还发现了可以绕过Office的保护模式的Microsoft Office安全功能绕过漏洞(CVE-2023-36413)，该漏洞已存在很长一段时间，最早使用该漏洞的样本可追溯到2017年。

2.6 3CXDesktop App 代码执行漏洞(CVE-2023-29059)

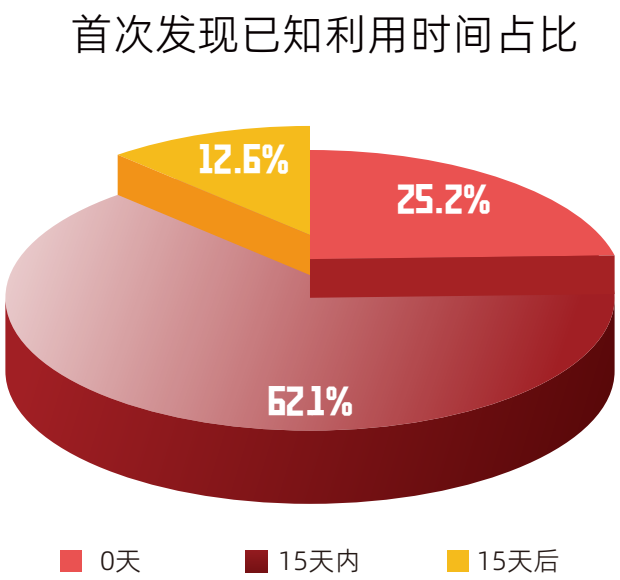
漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-29059	代码执行	9.6	是	未知	未知	已发现

3CXDesktopApp是由商业通信软件公司3CX开发的语音和视频会议专用自动交换机（PABX）企业呼叫路由软件。功能包括提供软件电话功能、支持多种通话功能、支持多种通话功能，提供的丰富语音通信能力和协作功能,提高办公效率和灵活性。

2023年3月22日国外用户在EDR上观测到3CXDesktop App试图向其他进程内存空间注入恶意代码，在构建3CXDesktop App时所使用的ffmpeg代码被投毒,导致在有合法签名的3CXDesktop App安装后加载的ffmpeg.dll中有恶意代码，该dll没有签名，ffmpeg.dll会加载dsdcompiler_47.dll中嵌入的shellcode，后续shellcode会加载dll并尝试从GitHub下载恶意代码并执行，收集受害者浏览器的历史记录等信息。后来经过调查，该事件为3CXDesktopApp被APT组织进行了供应链攻击，crowdstrike认为该APT组织是Labyrinth Chollima。

三、在野利用相关漏洞回顾

本节回顾了2023年部分影响较大的在野利用相关漏洞。2023年已知被利用的漏洞中，从漏洞公开与首次发现在野利用平均时间差值为35天，有25.2% 的高危漏洞在发布当天就被利用，62.1% 的高危漏洞在发布后15 天内被利用，公开时间与首次发现在野利用时间差值占比情况如图4-3所示所示：



△图4-3 漏洞公开时间与首次发现在野利用时间差

3.1 Atlassian Confluence Data Center and Server 权限提升漏洞 (CVE-2023-22515)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-22515	权限提升	10	是	已公开	已公开	已发现

Atlassian Confluence Data Center & Server 是 Atlassian 公司提供的一款企业级团队协作和知识管理软件。它旨在帮助团队协同工作、共享知识、记录文档和协作编辑等。

2023年10月4日，Atlassian修复Atlassian Confluence Data Center and Server 权限提升漏洞(CVE-2023-22515)，未经身份验证的远程攻击者可以用该漏洞来创建confluence管理员账户并访问Confluence实例。Atlassian发现该漏洞已被民族国家行为者积极利用。

3.2 Atlassian Confluence Data Center & Server 授权不当漏洞

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-22518	身份认证绕过	9.8	是	已公开	已公开	已发现

Confluence是由Atlassian开发的企业级团队协作和知识管理软件。旨在帮助团队协同工作、共享知识、记录文档和协作编辑等。

2023年10月31日Atlassian官方发布Atlassian Confluence Data Center & Server授权不当漏洞(CVE-2023-22518)公告修复此漏洞。该漏洞是由于Atlassian Confluence Data Center & Server滥用了Struts2的继承关系，导致远程攻击者可以无需认证即可控制并接管服务器。该漏洞利用对应用数据完具有较大的破坏性，会导致 Confluence 数据清空。PoC公开后黑客团伙于11月5日起对该漏洞进行大规模利用，Cerber勒索软件也通过该漏洞勒索受害组织。

2023年7月18日发布了针对该漏洞的补丁，在该漏洞爆出后持续监测到攻击者尝试利用该漏洞攻击Citrix Gateway。在2023年10月10日Citrix修复了CVE-2023-4966 NetScaler ADC 和 NetScaler Gateway 敏感信息泄露漏洞，该漏洞是在构造HTTP响应时，使用snprintf返回的长度作为参数读取内存，并且未验证长度范围，导致攻击者可以发送恶意请求读取Citrix Gateway内存中的已登录会话的cookie，可以使用该cookie登录Citrix Gateway后台，在2023年11月，LockBit勒索组织声称利用该漏洞成功在某银行内部部署了勒索软件。

3.3 Citrix Gateway 远程代码执行漏洞（CVE-2023-3519）

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-3519	代码执行	9.8	是	已公开	已公开	已发现
CVE-2023-4966	信息泄露	9.4	是	已公开	已公开	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。

由于Citrix Gateway在大型企业网络中的特殊性，其相关漏洞一直被相关攻击者所关注。在2023年6月，在野攻击者利用0day CVE-2023-3519 Citrix Gateway 远程代码执行漏洞攻击了某组织的NetScaler ADC设备并在该设备上部署Webshell，该漏洞是由于处理/gwtest/formssso接口的代码将用户输入拷贝到了栈缓冲区并且没有验证长度，导致栈溢出，可以利用栈溢出覆盖函数返回地址造成代码执行。随后citrix于2023年7月18日发布了针对该漏洞的补丁，在该漏洞爆出后持续监测到攻击者尝试利用该漏洞攻击Citrix Gateway。在2023年10月10日Citrix修复了CVE-2023-4966 NetScaler ADC 和 NetScaler Gateway 敏感信息泄露漏洞，该漏洞是在构造HTTP响应时，使用snprintf返回的长度作为参数读取内存，并且未验证长度范围，导致攻击者可以发送恶意请求读取Citrix Gateway内存中的已登录会话的cookie，可以使用该cookie登录Citrix Gateway后台，在2023年11月，LockBit勒索组织声称利用该漏洞成功在某银行内部部署了勒索软件。

3.4 Google libwebp 远程代码执行漏洞(CVE-2023-4863)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-4863	代码执行	8.8	是	已公开	已公开	已发现

Libwebp是一个开源的用于编码和解码WebP图像格式的C/C++库。它提供了一组函数和工具，用于将图像数据编码为WebP格式，并将WebP格式的图像解码为原始图像数据。Libwebp库可以作为其他程序的依赖库，用于添加WebP图像格式的支持。Libwebp应用范围非常广泛，被使用到各个软件上面。

2023年9月7日，Apple发布新版本修复了Apple ImageIO任意代码执行漏洞(CVE-2023-41064)，Citizen Lab宣布早在一周前就在华盛顿一国际办事处机构员工的设备上发现此漏洞利用。Apple ImageIO框架中包含了对WebP数据的支持，Apple随后向Google报告了Google libwebp远程代码执行漏洞(CVE-2023-4863),9月11日Google紧急发布WebP的安全修复，并指出Google已经意识到该漏洞存在在野利用。该漏洞是由于libwebp在解析WebP图片时霍夫曼编码表构造未正确校验数据大小，远程攻击者诱导受害者访问攻击者精心构造的恶意网站后，导致堆缓冲区溢出，从而执行恶意代码。

3.5 HTTP/2 协议拒绝服务漏洞(CVE-2023-44487)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-44487	拒绝服务	7.5	是	已公开	已公开	已发现

HTTP2是IETF开发的用来取代HTTP 1.1的新协议标准,主要目的是提高网页加载速度和减少延迟。由于新增了多路复用、二进制帧格式等特性，可以使用HTTP2并发发送或响应大量请求，并减少延迟和压缩请求。

在2023年10月10日，国外CDN厂商cloudflare发布博客，声称在2023年8月25日开始观测到有攻击者使用大量HTTP请求攻击受害者服务器，其峰值达到了每秒2亿次。该漏洞利用了HTTP/2协议中的特性：当客户端发送RST_STREAM帧时，流状态从半关闭转为关闭，释放一个流，客户端可以立即发起新请求占用这个释放的流。攻击者可以在短时间内可以并发发送大量请求而后发送RST_STREAM从而绕过服务器允许的并发流限制。通过这种方式，攻击者可以发送大量HTTP请求快速消耗服务器资源。

3.6 Progress MOVEit Transfer SQL注入漏洞(CVE-2023-34362)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-34362	代码执行	8.6	是	已公开	未公开	已发现

Progress MOVEit Transfer是一个功能强大且易于使用的安全文件传输解决方案,适用于各种规模的企业和组织。它可以大大简化企业的文件传输流程,确保文件传输的安全性和合规性。

在2023年5月CLOP勒索软件组织利用该漏洞在MOVEit Transfer Web服务上部署Web shell，随后在2023年5月31日，Progress Software发布了该漏洞的补丁，在10天内影响了大约130名受害者。该漏洞是由于在UserEngine.UserGetUsersWithEmailAddress函数中会拼接函数参数，攻击者可以通过制作恶意请求触发SQL注入，泄露存储的文件并在目标服务器上部署Web shell。

四、其它类别关键漏洞回顾

4.1 Fortinet FortiOS SSL-VPN 远程代码执行漏洞(CVE-2023-27997)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-27997	代码执行	9.8	是	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。Fortinet FortiOS SSL-VPN中存在堆溢出漏洞，允许未经身份验证的远程攻击者通过特制请求使设备远程崩溃或者在设备上执行任意代码。目前该漏洞的技术细节及EXP已在互联网公开。

4.2 Nacos 默认密钥身份认证绕过漏洞(QVD-2023-6271)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
QVD-2023-6271	身份认证绕过	9.4	是	已公开	已公开	未发现

Nacos是一个易于使用的平台，专为动态服务发现和配置以及服务管理而设计。可以帮助您轻松构建云原生应用程序和微服务平台。该系统通常部署在内网，用作服务发现及配置管理，历史上存在多个功能特性导致认证绕过、未授权等漏洞。

开源服务管理平台Nacos中存在身份认证绕过漏洞，由于Nacos默认未对token.secret.key进行修改，在鉴权开启的情况下，远程攻击者可以绕过密钥认证进入后台，造成系统受控等后果。目前，此漏洞细节及EXP已在互联网公开。

4.3 MinIO 信息泄露漏洞(CVE-2023-28432)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-28432	信息泄露	8.6	是	已公开	已公开	未发现

MinIO是一个高性能、与S3兼容的对象存储系统。它专为大规模的人工智能/机器学习、数据湖和数据库工作负载而设计。它采用软件定义的方式，在任何云端或本地基础设施上运行。

在集群部署的MinIO中，未经身份认证的远程攻击者通过发送特殊HTTP请求即可获取所有环境变量，其中包括MINIO_SECRET_KEY和MINIO_ROOT_PASSWORD，造成敏感信息泄露，最终可能导致攻击者以管理员身份登录MinIO。该漏洞在公开后，就被攻击者积极利用。

4.4 Windows 内核权限提升漏洞(CVE-2023-35359)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-35359	权限提升	7.8	是	已公开	已公开	未发现

Windows内核是Windows操作系统的核心组件，它是操作系统的底层部分，负责管理和协调计算机硬件和软件资源。内核提供了操作系统的基本功能和服务，包括进程管理、内存管理、设备驱动程序、文件系统、网络通信等。

2023年8月8日微软补丁日修复此漏洞，9月11日此漏洞技术细节与EXP在互联网上公开。具有低权限的本地攻击者利用此漏洞可以将权限提升至SYSTEM。用户被特权进程模拟时，内核允许其访问该用户当前的驱动器映射，攻击者可以欺骗特权进程从不受信任的位置加载配置文件和其他资源。多年来由此产生了许多问题，如CVE-2015-1644、CVE-2017-0213、CVE-2022-41073。微软在CVE-2023-35359的补丁中引入ObpUseSystemDeviceMap函数来强制文件打开操作使用进程的设备映射，而非模拟用户的设备映射，来解决此问题。

4.5 Glibc ld.so本地权限提升漏洞(CVE-2023-4911)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-4911	权限提升	7.8	是	已公开	已公开	未发现

GNU C Library项目为GNU系统和GNU/Linux系统以及其他许多使用Linux作为内核的系统提供了核心库。这些库提供关键的API，包括ISOC11、POSIX.1-2008、BSD、特定于操作系统的API等。这些API包括诸如open、read、write、malloc、printf、getaddrinfo、dlopen、pthread _ create、crypt、login、exit等基本工具。

GNU C库的动态加载器ld.so在处 GLIBC_TUNABLES环境变量时存在缓冲区溢出漏洞。允许本地攻击者在运行具有SUID权限的二进制文件时通过恶意的 GLIBC_TUNABLES 环境变量来提升普通权限至系统权限。该漏洞利用比较简单，且影响范围较大。在11月21日，CISA将该漏洞加入漏洞利用目录。

4.6 JumpServer未授权访问漏洞(CVE-2023-42442)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-42442	信息泄露	7.5	是	已公开	已公开	未发现

JumpServer是广受欢迎的国产开源堡垒机，是符合4A规范的专业运维安全审计系统。JumpServer帮助企业以更安全的方式管控和登录所有类型的资产，实现事前授权、事中监察、事后审计，满足等保合规要求。未经身份验证的远程攻击者利用该漏洞可以访问录像文件，远程获取到敏感信息。如果会话重播存储在S3或OSS或其他云存储中，则不受影响。

4.7 curl SOCKS5 堆溢出漏洞(CVE-2023-38545)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-38545	代码执行、拒绝服务	7.0	是	已公开	未公开	未发现

curl从1998年维护至今，已经成为HTTP请求命令行工具的事实标准，具有丰富的 Api 和 Abi(应用程序二进制接口)。curl被用于汽车、电视机、路由器、打印机、音频设备、手机、平板电脑、医疗设备、机顶盒、电脑游戏、媒体播放器等各种设备中，并且在超过200亿个安装中作为互联网传输引擎被成千上万的软件应用程序使用。

当使用socks5代理时，如果主机名大于255则curl会尝试使用本地解析代替远程解析，但没有按照预期工作，导致内存损坏，攻击者可以构造恶意主机名触发漏洞，成功利用该漏洞可造成代码执行。虽然该漏洞技术细节和PoC已公开，但该漏洞利用难度较大，影响有限。

4.8 Google Chrome 信息泄露漏洞(CVE-2023-4357)

漏洞编号	威胁类型	CVSS评分	漏洞威胁状态			
			细节是否公开	PoC状态	EXP状态	在野利用
CVE-2023-4357	信息泄露	5.4	是	已公开	未公开	未发现

Chrome是一款由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。

2023年8月16日Chrome发布新版本修复此漏洞，11月17日此漏洞技术细节与PoC在互联网上公开。由于Chromium项目集成了libxslt用于处理XSL，但它允许在XSL document()方法加载的文档内包含外部实体。未经身份验证的远程攻击者可以通过发送包含恶意XSL样式表和SVG图像的网站链接给受害者。受害者点击链接后，浏览器加载并解析恶意内容，攻击者可以读取本地文件。此漏洞还影响微信等其他使用Chromium内核的浏览器和应用程序。

05

通用处置建议及最佳实践

第五章

网络访问限制：
关闭网络设备管理接口，如Telnet、SSH、Winbox以及用于广域网（WAN）的 HTTP。使用强安全性的密码和加密来保护通信。

网络分段：
对设备的网络进行适当的分段，使其只能与支持其特定业务功能的设备通信。

密码保护：
强制使用复杂密码以及多因素身份验证（MFA），包括第三方服务帐户。同时考虑提供密码管理服务，以防止在浏览器中存储凭据。

账户清单：
对系统中的服务账户和其他特权账户进行清单盘点。确保它们遵循最小特权原则，并为其配置长而复杂的密码。限制这些账户在整个系统中的使用范围。

全面覆盖：
对所有设备和系统启用适当的防病毒软件或端点检测和响应工具，以提供对利用或威胁活动的最大可见性。有价值的检测用例需要端点日志记录或可见性记录。

资产清单：
确保拥有一个完整且定时更新的资产清单，并对所有使用设备和应用程序的版本号进行详细说明。

补丁管理:
检测软件升级，并将补丁应用于具有高严重性或已知在野利用漏洞的系统。

缓解措施：
如果无法立即应用补丁或补丁失效，可实施厂商提供的缓解措施。

最大可见性：
增加对易受攻击设备的日志记录。这将扩展现有警报的覆盖范围，并允许实施更多检测用例以捕捉异常行为或可疑的内部流量。

最新风险通知：
奇安信漏洞订阅服务可以帮助你从互联网海量的漏洞信息里筛选出真正有价值的那一部分，及时获得与组织相关的安全漏洞情报。

06

奇安信漏洞情报服务订阅

第六章

根据奇安信安全监测与响应中心大数据统计，每年监测到的漏洞信息高达数万条，平均每天新增上百条。如果依靠企业自身的安全部门处理这些漏洞势必会投入相当多的资源和成本，并且也容易遗漏一些不起眼却又危害极大的漏洞。面对井喷式的漏洞信息增长，传统“条文式”漏洞修补和防护的管理模式，已经无法适应数字化转型深入的要求，需要依靠外部可靠的漏洞情报对企业安全生产进行支持与管理。漏洞的处理从人工转向自动化成为必然趋势，企业安全能力体系及安全运行体系的升级，需要更加先进的漏洞情报体系进行支撑。

奇安信漏洞订阅服务可以帮助你从互联网海量的漏洞信息里筛选出真正有价值的那一部分，及时获得与组织相关的安全漏洞情报，同时为您提供可行的包含详细操作步骤的处置措施。这种服务会向您提供实时更新的、富化的漏洞信息报告，包括最新发现的漏洞、已知的漏洞和修补程序的建议。您可以根据报告中的内容迅速定位和排查自己的资产风险，及时采取有效的防范措施，更加高效的进行企业漏洞管理。奇安信漏洞情报服务具有如下优势：

一、最全面、最值得信赖的漏洞库。

收录1999年以来全量23万余条漏洞信息，涵盖通用网络产品漏洞、 工业控制漏洞、信创政务漏洞、车联网漏洞等多个领域。开源漏洞信息覆盖率达到100%，自研漏洞信息占比大于20%，核心信息完整率达到99%。

二、高效的漏洞情报运营。

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，对关键漏洞进行重点运营和持续跟踪，保证信息的准确性、及时性和处理优先级的可靠性。

三、及时的漏洞风险通知。

关键漏洞信息3小时内完成研判、定级和入库，保证用户能够第一时间查询获取。发生重大漏洞事件时，能够快速准确地识别、分析、定位漏洞，及时通过邮件、IM、API接口等方式将漏洞风险通知到客户，并给出可靠的缓解措施和修复方案。

四、提供技术细节深入分析与验证。

针对影响面巨大、威胁等级极高的漏洞提供独家深度分析报告，对漏洞进行深入分析和技术验证，披露漏洞技术细节、复现测试方法，基于漏洞深度分析提供更加详尽的处置步骤和自查检测方案。

五、灵活的API数据接口。

对外输出形式，不仅提供基于多维属性筛选的Web访问界面，还提供在线数据获取的API接口及离线数据包，用户可以根据自己需要集成到自有漏洞处理流程。

六、定制化漏洞应急响应服务。

支持基于厂商和软件名的推送订阅，可结合本地安全资产库，通过组件版本自动匹配受影响的资产，实现企业资产关联漏洞预警。提供定制化漏洞深度分析报告解答和技术咨询。

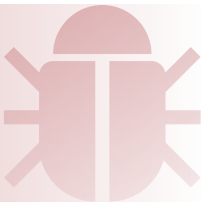
点击订阅

附录1：2023年APT活动相关漏洞列表

漏洞编号	事件发布时间	攻击事件披露	披露厂商	攻击组织
CVE-2023-42793	2023/12/14	APT29在大规模利用漏洞以瞄准JetBrains TeamCity	CISA	APT29
CVE-2023-42793	2023/12/13	APT29 疑似利用TeamCity的漏洞进行攻击	Fortinet	APT29
CVE-2021-44228 CVE-2021-21974 CVE-2022-0847	2023/12/5	土耳其Teal Kurma间谍组织及SnappyTCP恶意软件揭秘	PwC	Sea Turtle
CVE-2023-38831 CVE-2023-23397	2023/12/5	TA422组织向欧洲和北美地区发起大量攻击	Proofpoint	APT28
CVE-2023-23397	2023/12/4	来自俄罗斯的组织Forest Blizzard利用漏洞访问电子邮件帐户	未知	APT28
CVE-2023-38831	2023/11/21	蔓灵花组织投向国产办公软件的目光与winrar漏洞之触	深信服	蔓灵花
CVE-2023-46604	2023/11/17	Andariel组织利用Apache ActiveMQ漏洞安装NukeSped后门	AhnLab	Andariel Group
CVE-2021-44228	2023/11/10	Andariel组织滥用资产管理程序传播恶意软件	AhnLab	Andariel Group
CVE-2023-38831	2023/11/7	新兴APT组织DarkCasino的燎原之火，WinRAR零日漏洞的利用现状	绿盟	未知
CVE-2023-38831	2023/11/6	SideCopy 的多平台攻击：利用 WinRAR 零日和 Linux 变体 Ares RAT	Seqrite	SideCopy
CVE-2023-23397 CVE-2022-30190	2023/10/27	披露APT28攻击法国企业和大学等的TTP	CERT-FR	APT28
CVE-2023-38831	2023/10/26	矛头持续指向印度国防部，Sidecopy加入漏洞利用攻击队列	安恒	SideCopy

漏洞编号	事件发布时间	攻击事件披露	披露厂商	攻击组织
CVE-2020-12641 CVE-2021-44026 CVE-2020-35730	2023/6/20	APT28组织在一次间谍活动中使用了三个 Roundcube 漏洞	未知	APT28
CVE-2021-26084 CVE-2022-41040	2023/6/14	俄罗斯 GRU 赞助的新型威胁组织Cadet Blizzard	Microsoft	Cadet Blizzard
CVE-2023-34362	2023/6/9	MOVEit Transfer 深入研究	未知	Clop
CVE-2023-34362	2023/6/8	Clop可能自2021年就存在MOVEit 传输漏洞	未知	Clop
CVE-2023-34362	2023/6/7	MOVEit Transfer 被利用来删除窃取文件的 SQL Shell	SentinelOne	Clop
CVE-2023-27532	2023/4/26	在针对 Veeam 备份服务器的攻击中发现 FIN7 tradecraft	withsecure	FIN7
CVE-2017-6742	2023/4/18	APT28利用已知漏洞在思科路由器上进行侦察和部署恶意软件	NCSC	APT28
CVE-2022-27926	2023/3/30	Winter Vivern 利用已知的Zimbra漏洞攻击欧洲北约结盟政府的网络邮件门户	Proofpoint	WinterVivern
CVE-2017-8291	2023/2/14	RedEyes 黑客使用新的恶意软件从 Windows、手机窃取数据	AhnLab	Group123
CVE-2022-27925 CVE-2022-37042	2023/2/2	与朝鲜有关的黑客攻击印度医疗机构和能源部门	withsecure	Lazarus Group
CVE-2017-0199	2023/1/6	新APT组织Saaiwc Group针对东南亚军事、财政等多部门	安恒	Saaiwc

附录2：2023年风险通告（建议必修）漏洞列表



公开日期	漏洞名称	危险等级	是否在野利用	POC是否公开	EXP是否公开	技术细节是否公开	修复建议
2023-01-03	Fortinet FortiADC 命令注入漏洞(CVE-2022-39947)	高危	否	否	否	否	升级至7.0.2、6.2.4、 5.4.6及以上版本
2023-01-06	禅道项目管理系统远程命令执行漏洞 (QVD-2023-1953	极危	否	否	否	是	开源版升级至 18.0.beta2 及以上版本；企业版升级至 8.0.bate2 及以上版本；旗舰版升级至 4.0.bate2 及以上版本。
2023-01-10	Windows NTLM 权限提升漏洞(CVE-2023-21746)	高危	否	是	是	是	安装补丁
2023-01-10	Windows Backup Service 权限提升漏洞 (CVE-2023-21752)	高危	否	是	是	否	安装补丁
2023-01-10	Windows Ancillary Function Driver for WinSock 权限提升漏洞 (CVE-2023-21768)	高危	是	是	是	是	安装补丁
2023-01-13	Apache Shiro身份认证绕过漏洞(CVE-2023-22602)	高危	否	否	否	是	升级至 1.11.0
2023-01-14	pyLoad 远程代码执行漏洞(CVE-2023-0297)	极危	否	是	是	是	升级至安全版本
2023-01-18	Oracle WebLogic Server 远程代码执行漏洞 (CVE-2023-21839)	高危	是	否	是	否	安装补丁
2023-01-18	Zoho ManageEngine OnPremise 多款产品远程代码执行漏洞	极危	是	是	是	是	升级至安全版本
2023-01-18	Adobe Acrobat Reader 任意代码执行漏洞 (CVE-2023-21608)	高危	是	是	是	是	升级至：Acrobat DC >= 22.003.20310；Acrobat Reader DC >= 22.003.20310；Acrobat 2020 >= 20.005.30436；Acrobat Reader 2020 >= 20.005.30436。
2023-01-26	VMware vRealize Log Insight 远程代码执行漏洞(CVE-2022-31704)	极危	否	是	是	是	升级至安全版本
2023-01-26	VMware vRealize Log Insight 目录穿越漏洞 (CVE-2022-31706)	极危	否	是	是	是	升级至安全版本

公开日期	漏洞名称	危险等级	是否在野利用	POC是否公开	EXP是否公开	技术细节是否公开	修复建议
2023-01-26	VMware vRealize Log Insight 信息泄露漏洞 (CVE-2022-31711)	中危	否	是	是	是	升级至安全版本
2023-01-26	Argo CD身份认证绕过漏洞(CVE-2023-22482)	极危	否	否	否	否	升级至：Argo CD >= 2.6.0-rc5；Argo CD v2.5.x >= v2.5.8；Argo CD v2.4.x >= v2.4.20；Argo CD v2.3.x >= v2.3.14。
2023-01-26	Argo CD授权绕过漏洞 (CVE-2023-22736)	高危	否	否	否	否	更新至2.5.8/2.6.0-rc5
2023-01-29	QNAP QuTS hero 和 QTS SQL注入漏洞 (CVE-2022-27596)	极危	否	否	否	否	升级至：QTS >= 5.0.1.2234 build 2v0221201 ； QuTS hero >= h5.0.1.2248 build 20221215 and later。
2023-02-01	F5 BIG-IP 格式化字符串错误漏洞(CVE-2023-22374)	高危	否	是	否	是	1.通过对系统 iControl SOAP API 的访问限制为仅受信任的用户，可参考：https://my.f5.com/manage/s/article/K17459 2.若无需使用 iControl SOAP API，则可以通过将 iControl SOAP API 允许列表设置为空列表来禁用所有访问
2023-02-01	Jira Service Management Server 和 Data Center 身份认证绕过漏洞 (CVE-2023-22501)	极危	否	否	否	否	升级至安全版本
2023-02-01	IBM WebSphere Application Server 远程代码执行漏洞(CVE-2023-23477)	高危	否	否	否	否	V9.0.0.0 到 9.0.5.7：升级至 9.0.5.8 及以上版本；V8.5.0.0 到 8.5.5.19：升级至 8.5.5.20及以上版本。

注：以上仅展示部分漏洞，点击下载完整列表：

2023年风险通告（推荐必修）漏洞列表.csv

奇安信 | 奇安信 威胁情报中心

邮箱：ti_support@qianxin.com
电话：95015
官网：https://ti.qianxin.com
扫描关注我们的微信公众号