2022上半年

网络安全漏洞态势观察

中国信息安全测评中心

摘 要

2022 年上半年，网络安全漏洞形势依旧严峻，高危漏洞数量不断增长，漏洞利用渐趋隐蔽，融合叠加风险攀升，在野漏洞利用成为重大网络安全热点事件的风险点以及国家级 APT 活动的新手段。美欧国家从漏洞发现收集、修复消控、协同披露、出口管制等层面加大管控力度。

《2022 上半年网络安全漏洞态势观察》报告围绕漏洞数量变化趋势、漏洞危害、漏洞利用、漏洞管控等内容，把握总体形势，分析关键漏洞现实威胁，并在漏洞管控与综合治理、感知与预警、供应链安全与开源治理等方面提出对策建议。报告主要观点如下：

1、在漏洞数量方面，漏洞增长创新高，网络安全威胁持续加剧。漏洞总量环比增长达到 12%；危害程度较大漏洞仍然是热点，超高危漏洞占比超过 50%；微软、谷歌等美企大厂产品漏洞多发，持续成为安全研究焦点；开源软件漏洞频发，软件供应链安全风险凸显。

2、在漏洞利用方面，漏洞在野利用形势严峻，漏洞实战化趋势明显。漏洞 POC/Exploit 公开广泛传播，为漏洞实战化提供便利；在野漏洞利用不断增多，APT 组织漏洞利用异

常活跃；在野利用漏洞私有化、漏洞工具囤积严重。

3、在漏洞现实威胁方面，高价值漏洞“寄生”于多类目标，现实危害严重，影响持久。边界设备、操作系统、服务器软件、开源组件、协同办公软件、云原生、移动终端等目标对象漏洞在攻击活动中频繁现身；攻击者通过漏洞攻破网络“大门”、横向移动传播、获取控制权、破坏或窃取数据形成完整网络攻击组合拳；漏洞修复不完善引发“次生灾害”，历史漏洞重复利用或修复后再被突破，对漏洞治理提出更高要求。

4、在管控政策方面，漏洞披露与保留博弈深化。美欧根据形势不断制定或修订政策法规，加强漏洞资源管控；漏洞披露、共享在国家、企业间的“圈子化”趋势明显，漏洞战略地位凸显。

5、在对策建议方面，多措并举加强漏洞安全防范与保障成为当务之急。一是进一步强化国家级网络安全漏洞综合治理能力，加强漏洞管控统筹协调，提升漏洞资源共享共治水平。二是建设国家级漏洞感知与预警机制，提升漏洞发现与处置能力。三是积极推进 ICT 供应链安全治理，完善符合我国情的开源生态。

致 谢

感谢以下人员为本报告编制付出的辛勤劳动。

指导专家（按姓氏笔画排序，排名不分先后）

朱钱杭（启明星辰 Adlab）

张　超（清华大学）

张云海（绿盟科技天机实验室）

汪列军（奇安信威胁情报中心）

郑文彬（北京赛博昆仑科技有限公司）

龚　广（360 漏洞研究院）

隋　刚（知道创宇 404 实验室）

参编单位

中国信息产业商会信息安全产业分会

奇安信 威胁情报中心

360 漏洞研究院

北京知道创宇信息技术股份有限公司

目 录

一、聚米为山——从统计数据看漏洞态势

（一）超高危漏洞数量持续攀升，利用难度低危害大的漏洞仍是热点

2022 年上半年，无论从新增通用型漏洞总体数量来看，还是从危害较大的超危、高危漏洞分布情况来看，漏洞仍然是网络空间安全威胁的最大来源，漏洞数量持续增长，危害程度较大漏洞占比维持高位，一些容易被发现、利用难度不高但危害较大的漏洞类型成为热点。

据国家信息安全漏洞库（CNNVD）的统计数据[1]，2022 年上半年新增通用型漏洞信息共计 12466 条，按照超危、高危、中危、低危四种漏洞危害等级划分，其中：超危漏洞 1927 个，占比 16%；高危漏洞 4639 个，占比 37%；中危漏洞 5478 个，占比 44%；低危漏洞 422 个，占比 3%。漏洞危害等级分布如图 1 所示，从漏洞风险等级的分布来看，超高危漏洞占比较大，超过 2022 年上半年公开披露漏洞数量的 50%。

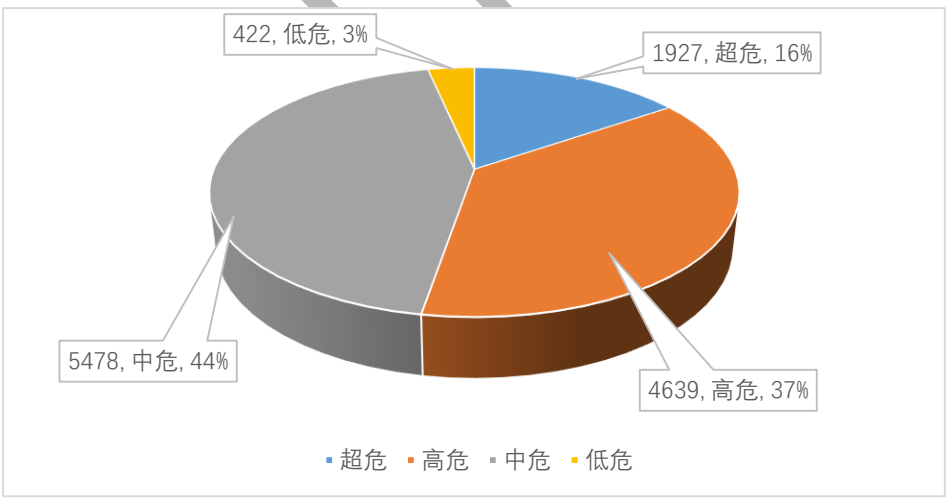


图 1 2022 年上半年新增漏洞风险等级分布

从漏洞类型来看，2022 年上半年新增漏洞中跨站脚本、缓冲区错误、SQL 注入、输入验证错误、代码问题等五种类型的漏洞数量最多，这也与美国 MITRE 发布的 2022 年 CWE 最危险的前 25 名软件漏洞类型（2022 Common Weakness

[1]https://www.cnnvd.org.cn

Enumeration（CWE）Top 25 Most Dangerous Software Weaknesses）[2]列表具有一致性。这些类型的漏洞通常很容易被发现、利用，并且可以让攻击者完全接管系统、窃取数据或阻止应用程序运行，危险性较大，是安全从业人员的重点关注对象。漏洞类型分布如图 2 所示。

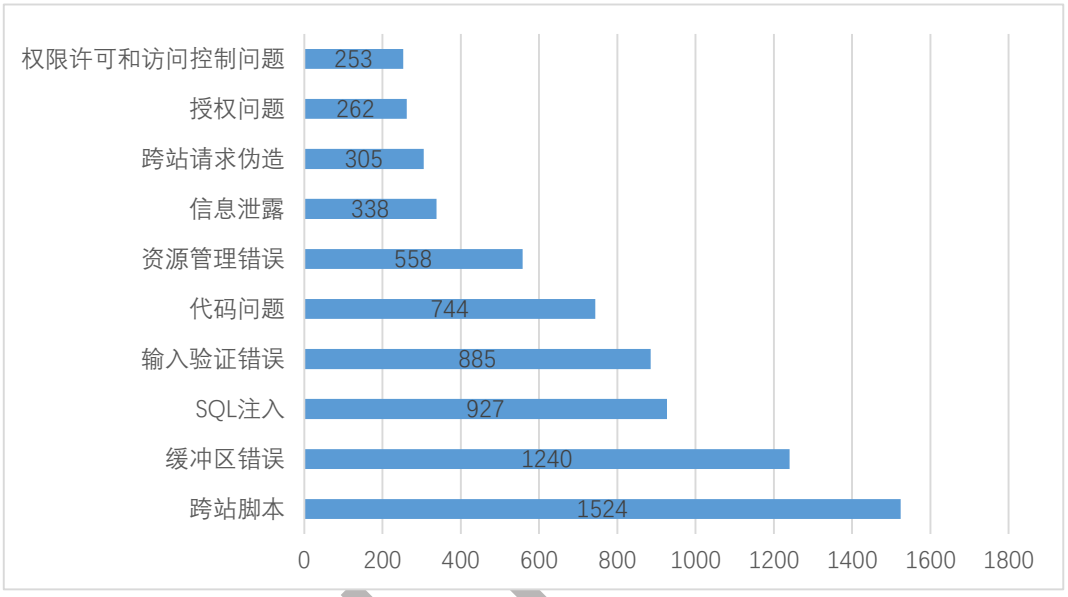


图 2 2022 年上半年新增漏洞威胁类型分布

（二）美企大厂产品漏洞多发，持续成为安全研究焦点

美国作为全球信息产业的领先国家，无论是在头部企业数量、技术创新水平方面，还是在其信息技术产品在全球应用、部署和使用量方面，均占据绝对优势。谷歌、微软、甲骨文、Adobe、思科等厂商的产品众多，应用广泛，成为 2022 年上半年受漏洞影响最为严重的厂商。这是因为美企大厂重视自身产品的安全问题，一方面利用自身力量不断挖掘发现产品安全漏洞，及时修复[3]；另一方面通过各种激励措施吸引外部安全研究人员参与漏洞分析，以提高产品的安全性[4]。此外，美企大厂均有较为规律的漏洞发布机制，定期发布安全公告和补丁信息，使其相关产品的漏洞受到重点关注。

基于 CNNVD 的漏洞收录数据，将 2022 上半年的 12466 条漏洞信息根据影响

[2] HTTP://cwe.mitre.ort/top25/archive/2022/2022_cwe_top25.html
[3] https://google.github.io/oss-fuzz
[4] https://microsoft.com/en-us/msrc/bounty?rtc=1

厂商进行分类统计，如表 1 所示。漏洞数量排名前 10 家厂商中，8 家为美国企业，相关产品涉及操作系统、应用软件、数据库软件、网络设备以及开源软件等。

表 1 2022 年上半年新增漏洞影响厂商 TOP10

序号	厂商名称	漏洞数量	所占比例
1.	WordPress（美）	904	7.25%
2.	谷歌（美）	622	4.99%
3.	微软（美）	487	3.91%
4.	甲骨文（美）	259	2.08%
5.	Adobe（美）	213	1.71%
6.	IBM（美）	206	1.65%
7.	Tenda（中）	170	1.36%
8.	苹果（美）	169	1.36%
9.	思科（美）	168	1.35%
10.	三星（韩）	160	1.28%

（三）供应链安全风险凸显，开源软件漏洞“风头正劲”

“太阳风”供应链漏洞攻击的余温未退，引起网络空间更大安全恐慌的 Log4j 漏洞又汹汹来袭，供应链漏洞正成为网络空间的新风险。2022 年上半年，由于开源软件和组件的应用越来越广泛，以及供应链安全的热度不断提升，这类软件的漏洞受到越来越多的关注。

新思科技基于对 17 个行业的 2409 个代码库进行审计发现[5]，97%的代码中存在开源组件漏洞，81%的代码库中包含至少一个已公开开源组件漏洞，49%的代码库中包含至少一个高风险漏洞。以被广泛使用的 jQuery 开源组件为例，43%的被审计代码库使用了 jQurey 组件，该组件中的漏洞会对这些代码库的安全产生直接或间接影响。

[5] https://synopsys.com/zh-cn/software-integrity/resources/anslyst-reports/open-source-security-risk-analysis.html

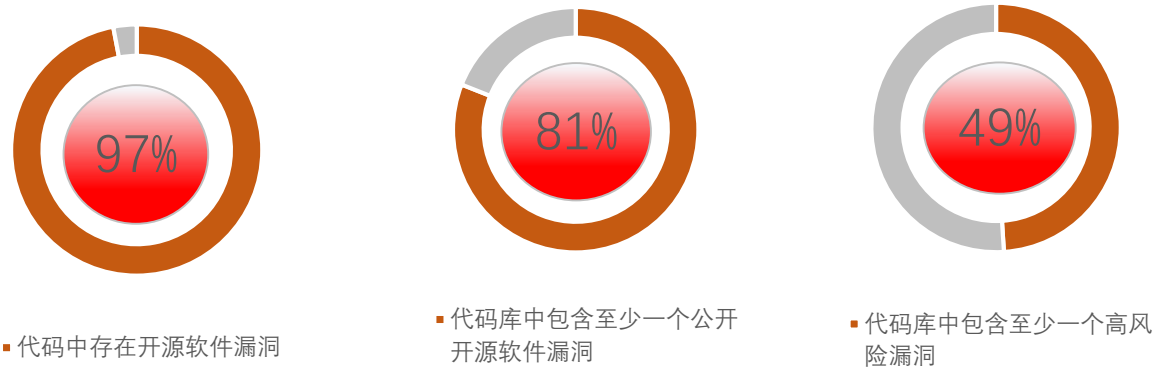


图 3 开源代码库漏洞情况

以“Spring4Shell”(CNNVD-202203-2514/CVE-2022-22965)漏洞事件为例，自 2022 年 3 月 29 日被小范围公开后，其影响面迅速扩大，国外将其命名为“Spring4Shell”。2022 年 4 月 4 日，美国网络安全和基础设施安全局（CISA）将该漏洞添加到其已知利用漏洞目录后，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。趋势科技（Trend Micro）在 2022 年 4 月即发现该漏洞大量在野传播，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[6]。此漏洞可以说是 2022 年上半年热度最大，也是近几年来最严重的网络安全威胁之一。

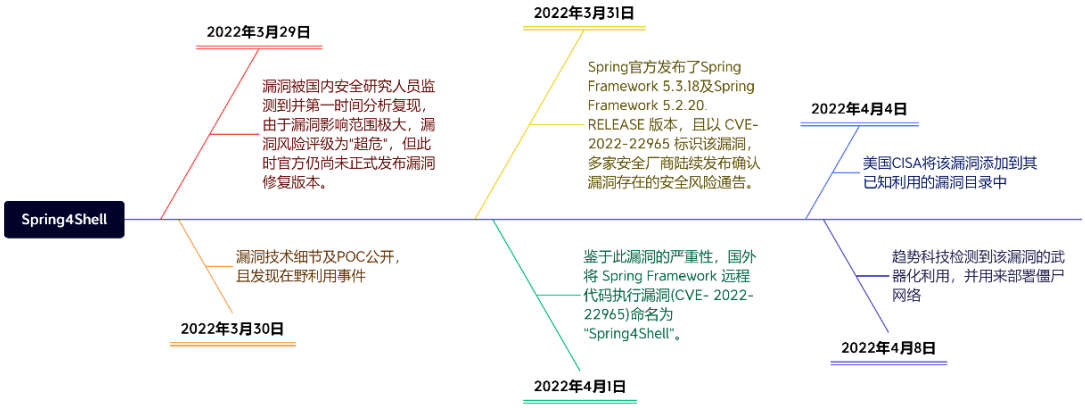


图 4“Spring4Shell”漏洞事件进展

[6] https://trendmicro.com/en-us/research/22/d/cve-2022-22965-analyzing-the-exploitation-of-spring4shell-vulner.html

（四）漏洞 POC/Exploit 信息增加，漏洞利用实战化态势明显

漏洞 POC 为漏洞验证、复现提供了样本数据，公开的漏洞 POC/Exploit 信息增加了漏洞被广泛利用的风险，尤其是有效的 Exploit 信息，将漏洞利用进一步推向实战化，为攻击者利用此类漏洞发起攻击提供了极大便利。

经奇安信监测发现，2022 年上半年互联网公开披露漏洞 POC/Exploit 的数量为 1876 个。在这些新增的漏洞 POC/Exploit 中，涉及 2022 年新增漏洞（CVE-2022-XXXX）的数量为 875 个，占 2022 年公开漏洞细节漏洞总量的 47%[7]，占 2022 年上半年新增漏洞的 7%。具体统计情况如图 5 所示。

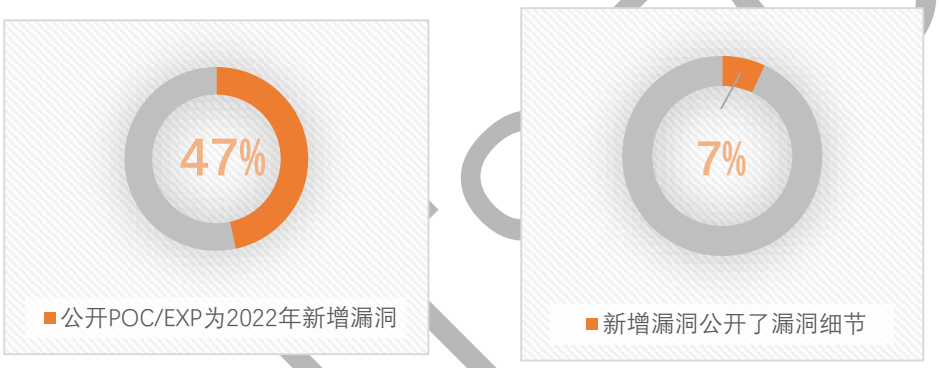


图 5 2022 年上半年公开披露 POC/Exploit 情况

（五）在野漏洞利用不断增多，APT 组织囤积漏洞工具蓄势待发

漏洞利用仍是 APT 组织进行网络攻击的主要手段，操作系统漏洞、终端应用软件漏洞、网络设备漏洞、WEB 应用漏洞等在野利用情况均有增无减，其大量漏洞攻击工具被 APT 组织或个人攻击者私下掌握，漏洞工具囤积情况严重。

经奇安信威胁监测发现，2022 年上半年新增在野利用漏洞数量 475 个，其中公开披露 POC\EXP\漏洞细节的漏洞共有 348 个，超过 70%的漏洞 POC\EXP\漏洞细节已经在互联网上流传[7,8]，并被某些 APT 组织或者恶意软件团伙频繁使用，这些漏洞存在较大的现实威胁，需尽快修复；涉及 2022 年新增漏洞的数量为 43 个，0day 在野利用漏洞数量为 18 个[9]。新增在野利用漏洞中，Windows、Linux、macOS/iOS、Android 等操作系统相关漏洞共计 90 个，网络设备漏洞共计 82 个，

[7] 奇安信威胁情报
[8] HTTPS:// cisa.gov/known-exploiter-vulnerabilities-catalog
[9] HTTPS://googleprojectzero.github.io/0day-in-the-wild/rca.html

浏览器、办公软件等终端软件相关漏洞共计 92 个，这三类漏洞占所有新增在野利用漏洞近 55%。在野利用漏洞分布情况如图 6 所示。

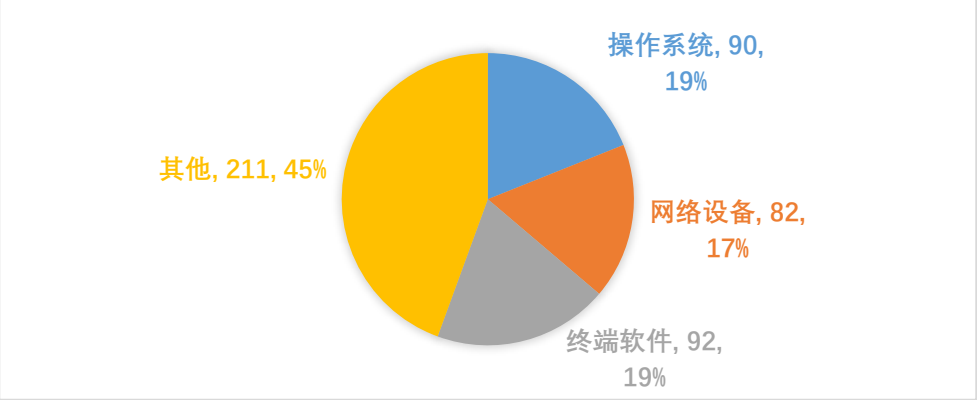


图 6 2022 年上半年在野利用漏洞分布情况

据知道创宇监测数据显示，2022 年上半年最受关注十大 Web 漏洞被国内外黑客大量用于对我境内目标的攻击活动，单一漏洞最大利用量超过 8000 万次[10]。

表 2 2022 年上半年最受关注的十大 Web 漏洞

序号	漏洞名称	漏洞编号	利用量
1	Apache Log4j 远程代码执行漏洞	CNNVD-202112-799 (CVE-2021-44228)	84,371,231
2	IBM WebSphere Portal SSRF	-	2,879,741
3	Atlassian Crowd 远程代码执行漏洞	CNNVD-201905-1031 (CVE-2019-11580)	1,149,725
4	Apache Druid 任意文件读取漏洞	CNNVD-202109-1676 (CVE-2021-36749)	1,039,259
5	帆软报表 V8 任意文件读取漏洞	CNVD-2019-41405	1,028,775
6	若依管理系统任意文件读取漏洞	CNVD-2021-15555	929,448
7	Apache Flink 目录遍历漏洞	CNNVD-202101-271 (CVE-2020-17519)	845,748
8	泛微 OA 前台任意文件下载漏洞	-	831,286
9	Fortinet FortiOS 路径遍历漏洞	CNNVD-201905-1026 (CVE-2018-13379)	776,811
10	Spring4Shell 远程代码执行漏洞	CNNVD-202203-2514 (CVE-2022-22965)	729,057

APT 组织在攻击活动中利用 1day 或 Nday 已成为标配动作，针对重点目标甚至不惜使用 0day 进行渗透。2022 年上半年，360 公司监测发现全球范围内 APT

[10] 知道创宇-创宇安全智脑

组织利用的漏洞近 50 个，涉及组织 30 余个，360 高级威胁研究院于 2022 年 2 月在全球范围内率先捕获到 APT-C-06（Darkhotel）组织利用 Firefox 浏览器的 2 个在野 0day 漏洞（CNNVD-202203-501、CNNVD-202203-503）针对特定目标进行水坑攻击[11]。2022 年上半年有威胁情报团队披露，具有俄罗斯情报部门背景的高级持续性威胁组织 APT28，向乌克兰用户投放恶意文档，目的是窃取储存在浏览器中的用户凭据，使用的漏洞为在 Microsoft Windows 支持诊断工具 (MSDT)中发现的 0day 漏洞 CNNVD-202205-4277(CVE-2022-30190)，该漏洞也称为“Follina”。谷歌威胁分析团队在 2022 年 6 月发布公告[12]称，他们在 2021 年发现的 9 个 0day 漏洞中有 7 个漏洞正在被恶意软件团伙积极利用，并详细说明了 RCS Labs 恶意软件团伙使用 CNNVD-202108-1974(CVE-2021-30883)、CNNVD-202108-2086(CVE-2021-30983)等 6 个发布在苹果越狱社区的 0Day 漏洞，针对意大利和哈萨克斯坦的移动用户发起恶意软件攻击的利用细节。

据公开数据显示，2022 年上半年，大量在野利用漏洞被多个 APT 组织在大规模攻击活动中使用，既有 5 年甚至 10 年以上的“骨灰级”漏洞，也有“新鲜出炉”的 0day 漏洞，涉及操作系统、网络设备及终端软件等目标产品。具体如表 3 所示：

表 3 APT 活动相关漏洞列表

漏洞编号	影响产品	利用代码是否公开	涉及的 APT 组织	攻击事件披露厂商
CNNVD-202203-501（CVE-2022-26485）	Firefox 浏览器	否	APT-C-06（Darkhotel）	360[11, 13]
CNNVD-202203-501（CVE-2022-26486）				
CNNVD-202112-799 (CVE-2021-44228)	Apache Log4j	是	APT35；Charming Kitten；TA453；Phosphorus	checkpoint[14]
CNNVD-201704-692 (CVE-2017-0199)	Microsoft Office	是	BlueNoroff；Lazarus	securelist[15] 奇安信[16]
CNNVD-201711-508 (CVE-2017-11882)	Microsoft Office	是	APT-35； SectorE02； 摩诃草； Hangover；Patchwork；白象；APT-	welivesecurity[17] 奇安信[18]

[11] 360 高级威胁研究院
[12] https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/
[13] https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/
[14] https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/
[15] https://securelist.com/the-bluenoroff-cryptocurrency-hunt-is-still-on/105488/
[16] https://ti.qianxin.com/blog/articles/analysis-of-the-lazarus-group-attacks-on-korean-companies/
[17] https://www.welivesecurity.com/2022/01/18/donot-go-do-not-respawn/
[18] https://ti.qianxin.com/blog/articles/analysis-of-the-attack-activities-of-patchwork-using-the-

			Q-36	
CNNVD-201204-122 (CVE-2012-0158)	Microsoft Windows	是	ModifiedElephant	sentinelone[19]
CNNVD-201403-433 (CVE-2014-1761)	Microsoft Office	是		
CNNVD-201311-073 (CVE-2013-3906)	Microsoft Windows	是		
CNNVD-201504-253 (CVE-2015-1641)	Microsoft Office	是		
CNNVD-202107-741 (CVE-2021-34473)	Microsoft Exchange	是	APT35；CharmingKitten；TA453；Phosphorus；COBALT；ILLUSION；ITG18；Newscaster	thedfirreport[20]
CNNVD-202107-740 (CVE-2021-34523)	Microsoft Exchange	是	APT35；Charming Kitten；TA453；Phosphorus；COBALTILLUSION；ITG19；Newscaster	
CNNVD-202105-543 (CVE-2021-31207)	Microsoft Exchange	是	APT35；Charming Kitten；TA453；Phosphorus；COBALTILLUSION；ITG20；Newscaster	
CNNVD-202203-2097 (CVE-2022-24934)	WPS Office	否	Operation Dragon Castling	avast[21]
CNNVD-202202-1153 (CVE-2022-0609)	Google Chrome	否	Operation Dream Job；Operation AppleJeus	谷歌[22]
CNNVD-202006-1830 (CVE-2020-15368)	ASRock RGB Driver	是	未知	CISA[23]
CNNVD-201711-508 (CVE-2017-11882)	Microsoft Office	是	Bitter；T-APT-17	talosintelligence[24]
CNNVD-201801-355 (CVE-2018-0802)	Microsoft Office	是		
CNNVD-201801-394 (CVE-2018-0798)	Microsoft Office	否	Bitter；T-APT-17；Tonto Team；CactusPete；Earth Akhlut	Talosintelligence，sentinelone[25]
CNNVD-201910-954 (CVE-2019-3010)	Oracle Solaris	是	DecisiveArchitect	Crowd Strike[26]
CNNVD-202203-2229 (CVE-2022-1040)	Sophos Firewall	否	DriftingCloud	volexity[27]，sophos[28]
CNNVD-202205-4277 (CVE-2022-30190)	Microsoft Windows	是	APT28；Sofacy；Fancy Bear	malwarebytes[29]

documents-of-relevant-government-agencies-in-pakistan-as-bait/

[19] https://www.sentinelone .com/labs/modifiedelephant-apt-and-a-decade-of-fabricating-evidence/

[20] https://thedfirreport .com/2022/03/21/apt35-automates-initial-access-using-proxyshell/

[21] https://decoded.avast .io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies/

[22] https://blog.google/threat-analysis-group/countering-threats-north-korea/

[23] https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

[24] https://blog.talosintelligence .com/2022/05/bitter-apt-adds-bangladesh-to-their.html

[25] https://www.sentinelone .com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/

[26] https://www.crowdstrike .com/blog/how-to-hunt-for-decisivearchitect-and-justforfun-implant/

[27] https://www.volexity .com/blog/2022/06/15/driftingcloud-zero-day-sophos-firewall-exploitation-and-an-insidious-breach/

[28] https://news.sophos .com/en-us/2022/06/15/sophos-uncovers-how-apt-groups-carried-out-highly-targeted-attack/

[29] https://blog.malwarebytes .com/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine/

二、见微知著——从“明星”漏洞看现实威胁

2022 年上半年，针对操作系统、开源组件、协同办公软件、云原生及虚拟化软件、网络设备、移动平台等目标对象，均曝光了多个具有较大影响的漏洞，并在实际网络攻击中产生了较大现实威胁。通过对 2022 年上半年披露的 29 个“明星”关键漏洞的分析发现，76%的关键漏洞公开了漏洞细节，或披露了漏洞 POC，或有漏洞利用代码公开传播，41%的关键漏洞发现在野利用的情况，具体情况如图 7 所示。

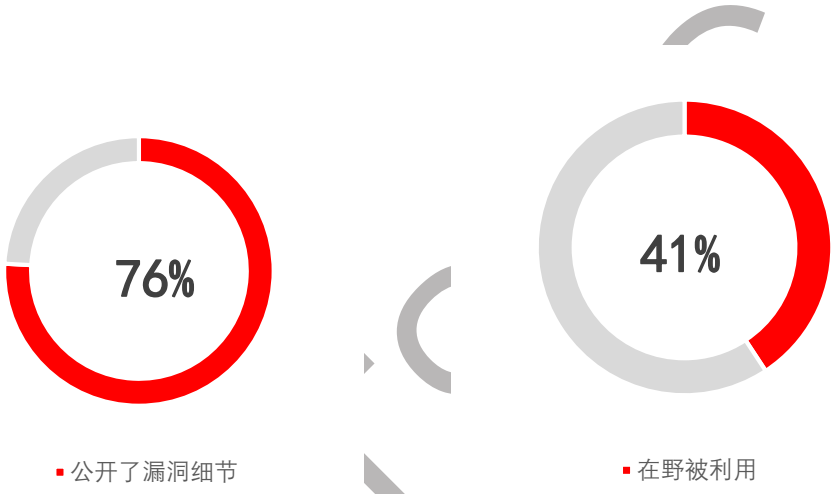


图 7 2022 年明星漏洞统计情况

（一）操作系统及服务端漏洞助攻击者获得较高控制权限

操作系统内核及服务端软件一直是网络攻击的传统目标，其相关漏洞也一直占据着重要位置。2022 年上半年，Windows、Linux 等操作系统及所属服务端软件爆出多个典型关键漏洞，且漏洞 POC 或 Exploit 代码在互联网上广泛传播，攻击者利用此类漏洞能够获取对目标的较高控制权，进而为实施更深层次的网络渗透提供更大的便利和可能。

表 4 操作系统及服务端软件“明星”漏洞

目标类型	受影响目标	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
操作系统及服务器	Windows Remote Desktop	CNNVD-202203-691（CVE-2022-21990）	代码执行	8.8	是	已公开	未知	未知
	Windows AD 域	CNNVD-202205-2850（CVE-2022-26923）	权限提升	8.8	是	已公开	已公开	未知
	Windows Network	CNNVD-202205-2781	代码执行	9.8	是	已公开	未知	未知

	File System	（ CVE-2022-26937）						
	Windows HTTP 协议栈	CNNVD-202201-779（ CVE-2022-21907）	代码执行	9.8	是	已公开	未知	未知
	Windows RPC	CNNVD-202204-3019 (CVE-2022-26809)	代码执行	9.8	是	未知	未知	未知
	Exchange Server	CNNVD-202201-734（CVE-2022-21846）	代码执行	9.0	否	未知	未知	未知
		CNNVD-202201-730（CVE-2022-21855）	代码执行	9.0	否	未知	未知	未知
		CNNVD-202201-731（CVE-2022-21969）	代码执行	9.0	否	未知	未知	未知
	Linux DirtyPipe	CNNVD-202203-522（CVE-2022-0847）	权限提升	7.8	是	已公开	已公开	未知
	Linux Polkit	CNNVD-202201-2343（CVE-2021-4034）	权限提升	7.8	是	已公开	已公开	未知

在 Windows 操作系统方面，2022 年上半年出现了 Remote Desktop Client 远程代码执行漏洞(CNNVD-202203-691)、Windows AD 域权限提升漏洞（CNNVD-202205-2850）、Windows Network File System 远程代码执行漏洞(CNNVD-202205-2781)、HTTP 协议栈远程代码执行漏洞(CNNVD-202201-779) 等重要漏洞。其中，CNNVD-202203-691 漏洞存在于 Windows 远程桌面，几乎影响了从 Windows7 到 Windows11，从 Windows server2008 到 Windows server2019 的大部分操作系统版本。**值得注意的是，该漏洞的 POC 代码在微软发布安全公告之前就已经在互联网上公开传播**。CNNVD-202205-2850 是一个域内权限提升漏洞，在安装了活动目录证书服务（Active Directory Certificate Service，ADCS）的默认活动目录环境中，利用该漏洞可以将低权限的用户升级为域管理员权限，从而完全控制域，该漏洞影响的 ADCS 服务常应用于企业级网络内，**是攻击者进行渗透、横向移动和数据窃取的一个关键目标**。该漏洞由趋势科技 0day 计划（Zero Day Initiative，ZDI）的研究员报告给微软公司，微软在 5 月 10 日发布了安全补丁进行修复，随后 5 月 11 日 ZDI 的研究员就公开了漏洞细节及漏洞 POC。CNNVD-202205-2781 影响 Windows 网络文件系统（Network File System，NFS），远程攻击者可通过向 NFS 服务器发送特制数据包来利用此漏洞，从而在目标系统上执行任意代码。目前，**此漏洞在微软发布安全补丁之后，ZDI 的研究人员在互联网上公布了该漏洞的细节及 POC 代码**。CNNVD-202201-779 是影响 Windows 内核驱动程序的远程代码执行漏洞，由于 Windows 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而引起。虽然该漏洞仅影响 Windows10、Windows11、Window Server2019 和 Windows Server2022 的部分版本，但由于影响的均是服务端，且微软在公告中提示**该漏洞“可蠕虫化”，即**

无需用户交互便可通过网络进行自我传播，因此该漏洞仍然危害较大，应引起重视。Windows RPC Runtime 远程代码执行漏洞(CVE-2022-26809)是由于 RPC Runtime 在处理网络数据的过程中缺乏校验，存在整数溢出问题，可允许攻击者绕过后面的判断逻辑进行越界读写。攻击者**无需身份认证和用户交互**，只需通过向目标系统发送特制的 RPC 数据包即可利用此漏洞，允许攻击者在服务器端以与 RPC 服务相同的权限执行任意代码。

在 Linux 操作系统方面，2022 年上半年出现了 Linux DirtyPipe 内核本地权限提升漏洞(CNNVD-202203-522) 和 Linux Polkit 本地权限提升漏洞(CNNVD-202201-2343)两个影响较大的典型关键漏洞，这两个漏洞均存在公开的 Exploit，攻击者可基于已经公开的 Exploit 较为容易的开发出具有实战效果的攻击程序。其中，CNNVD-202201-2343 是一个影响 Linux 近 13 年的漏洞，该漏洞存在于几乎所有主流版本的 Linux 操作系统的默认配置中，攻击者利用该漏洞能够从普通权限提升到 root 权限，目前该漏洞的 Exploit 信息已经在互联网上公开，由于该漏洞利用难度较低，因此**被公认为 2022 年最好用的权限提升漏洞**。

在服务端软件方面，Microsoft Exchange Server 作为在全球企业及学术机构中应用最为广泛的电子邮件服务器软件之一，一直都是黑客攻击的首要目标。因邮件服务器中存储大量数据，如果黑客发起攻击，可能导致用户敏感数据泄露，给企业和用户带来重大损失。2022 年上半年，微软公开披露了多个该软件的远程代码执行漏洞，包括：CNNVD-202201-734、CNNVD-202201-730 以及 CNNVD-202201-731 等。其中，**CNNVD-202201-734 被微软标记为紧急漏洞，CNNVD-202201-730、CNNVD-202201-731 风险等级为重要**。虽然目前没有公开发现这些漏洞的 POC 或 Exploit，但此类漏洞仍然值得重点关注。

（二）开源组件及软件漏洞波及范围广

开源软件中的安全漏洞在现实网络攻击中为攻击者提供了新的攻击思路，拓展了攻击面，降低了攻击难度，攻击者通过利用开源软件漏洞即可引发软件供应链全过程的“链式反应”，周边直接或间接关联系统均会受到影响，甚至可能会出现“网状蔓延”的态势，攻击影响可成倍甚至呈爆炸式放大。

从俄乌冲突中知名开源组件 Node-ipc 被供应链投毒植入恶意代码，到影响

JAVA 生态的 Spring 框架被披露存在严重漏洞甚至被广泛利用，再到 Apache Struts2 漏洞不止，2022 年开源软件漏洞风头不减，仍是影响网络安全的重要因素。同时，由于开源软件天然的代码可获得性，曝露出的漏洞极易被快速开发出 POC 或者 Exploit，在网络攻击中作为网络武器被广泛使用。

表 5 开源组件及软件“明星”漏洞

目标类型	受影响目标	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
开源组件	Apache Struts2	CNNVD-202204-3223（CVE-2021-31805）	代码执行	9.8	是	已公开	已公开	未知
	Zabbix	CNNVD-202201-2514（CVE-2021-46088）	代码执行	7.2	是	已公开	已公开	未知

阿帕奇基金会（Apache）是全球最大的开源软件组织，负责管理运维数十个开源软件项目。2022 年上半年，Apache Struts2 开源框架及 Apache APISIX 开源组件均披露了较为严重的安全漏洞。其中，Apache Struts2 作为全球最流行的轻量级 WEB 框架之一，在互联网上对外开放的服务数量达到近 500 万个，历史上该开源框架曾经曝出很多高危漏洞，2022 年上半年该框架又曝出远程代码执行漏洞(CNNVD-202204-3223)，虽然该漏洞编号为 2021 年，但实际在 2022 年 4 月才被公开披露。该漏洞的产生是由于其前一个漏洞 CNNVD-202012-449（S2-61）修复不完整导致的，攻击者可通过构造恶意的 OGNL 表达式触发漏洞，从而实现远程代码执行。

在开源软件及解决方案方面，Zabbix 作为一款应用广泛的具有分布式系统监视以及网络监视功能的企业级开源解决方案，能监视各种网络参数，保证服务器系统的安全运营。该软件被披露存在远程代码执行漏洞(CNNVD-202201-2514)，任何具有“Zabbix Admin”角色的攻击者都可以在对应服务器上运行自定义 shell 脚本，并获取控制权。该漏洞虽然利用难度较高，但若管理员身份凭证泄漏，将影响企业中所有部署 Zabbix Agent 的服务器，影响面极其广泛。目前，**该漏洞的 Exploit 代码已经在互联网上公开传播。**

（三）协同办公软件漏洞危及企业运行

远程办公、协同办公、在线会议等软件因新冠疫情原因需求猛涨，大量软件、

服务曝露于互联网上。由于这些应用软件及系统深度融合了企业的运作及生产经营，甚至承载企业大量的敏感信息，它们存在的漏洞、曝露的安全风险会造成重要敏感信息泄露，严重的会危及企业的正常运行及生存。2022 年，多款协同办公软件爆出高危漏洞，既有在全球部署和使用的大型软件系统，又有我国内本土软件，其中多个漏洞均已发现被攻击者在野利用。

表 6 协同办公软件明星漏洞

目标类型	受影响目标	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
协同办公软件	Windows MSDT	CNNVD-202205-4277（CVE-2022-30190）	代码执行	7.8	是	已公开	已公开	已发现
	MS SharePoint Server	CNNVD-202202-580（CVE-2022-22005）	代码执行	9.0	否	未知	未知	未知
		CNNVD-202205-2730（CVE-2022-29108）	代码执行	9.0	否	未知	未知	未知
	Atlassian Confluence	CNNVD-202206-442（CVE-2022-26134）	代码执行	9.8	是	已公开	已公开	已发现
	向日葵	CNVD-2022-10270	代码执行	9.8	是	已公开	未知	已发现
	钉钉	NA	代码执行	8.8	是	已公开	未知	已发现

2022 年上半年影响办公类软件最严重的漏洞之一就是微软 Windows 支持诊断工具 MSDT (Microsoft Support Diagnostics Tool) 远程代码执行漏洞(CNNVD-202205-4277)。MSDT 是 Windows 系统中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，该漏洞影响了微软 Office 2019、Office 2021 以及 Office 365 的 5 月版本。由于该漏洞被检测出 0day 在野利用，迫于漏洞的影响力及关注度，微软于 2022 年 5 月 30 日发布紧急通告给出了相应缓解措施，从而在一定程度缓解了该漏洞影响，并最终于 6 月补丁日得到修复。虽然该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，但**由于该漏洞的危害程度及影响范围，在实际网络攻击中仍作为攻击工具被广泛应用**。

在协同办公软件及系统方面，企业级软件 Microsoft SharePoint Server 及 Atlassian Confluence 均出现严重漏洞。其中，Microsoft SharePoint Server 公开了多个远程执行代码漏洞，CNNVD-202202-580 和 CNNVD-202205-2730 被微软标记为 **“更有可能被利用**（Exploitation More Likely）”，这些漏洞允许经过身份验证的攻击者在目标服务器上以 SharePoint Web 服务帐户权限执行任

意代码。SharePoint 软件系统拥有超过 200,000 个组织和 1.9 亿人的用户，因此漏洞的影响范围极广。Atlassian Confluence 是一个专业的企业知识管理与协同软件，主要用于构建企业知识库。2022 年上半年，Atlassian Confluence Server 及 Confluence Data Center 中曝出严重的远程代码执行漏洞(CNNVD-202206-442)，利用该漏洞，任意用户仅通过发送一条 HTTP GET 请求即可在目标服务器上执行任意代码，获取服务器权限。由于**该漏洞利用难度极低**，之后披露出多起攻击事件均利用该漏洞进行攻击。

在我国本土协同办公软件方面，向日葵远程控制软件和钉钉软件均出现较为严重的安全漏洞。其中，向日葵远程控制软件是一款免费的集远程控制电脑手机、远程桌面连接、远程开机、远程管理、支持内网穿透于一体的远程控制管理工具软件。2022 年 2 月，**该软件 Windows 版本被曝光存在远程命令执行漏洞，并已经发现在野利用**，由于很多企业的安全意识不足，将向日葵的接口主动曝露在公网，在漏洞公开后，大量企业受到了攻击，包括挖矿、勒索、僵尸网络等，且漏洞影响的对应版本不能通过自动升级的方式进行软件升级，这更是给了不法分子充足的时间进行恶意攻击，从而使企业遭受更大损失。钉钉（DingTalk）是阿里巴巴集团专为中小企业打造的沟通和协同的多端平台。2022 年 2 月，钉钉远程代码执行漏洞被公开[30]，并已发现在野利用，攻击者通过将恶意链接发送至受害者，诱使受害者点击该链接，钉钉即会获取恶意链接指向的网页内容并用内置浏览器渲染，从而触发漏洞，在受害者电脑上远程执行代码。通过该漏洞，**攻击者可将受害者的机器当作跳板，用来攻击企业内网，从而获取企业内部数据，使企业遭受不必要的损失**。

（四）云原生及虚拟化漏洞影响云基础设施安全

随着云计算技术的不断和发展，云原生的安全引起了业界的广泛关注，云原生相关组件的漏洞，威胁到云基础设施的整体安全，甚至会渗透并威胁到云上业务应用的安全。2022 年，云原生开源组件及引擎、虚拟化软件等均爆出多个关键漏洞，且相关漏洞利用代码被广泛传播，在多起网络安全事件中发现漏洞被利用，严重危害了相关云平台的安全。

[30] https://github.com/crazy0x70/dingtalk-RCE

表 7 云原生及虚拟化软件“明星”漏洞

目标类型	受影响目标	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
云原生及虚拟化	Apache APISIX	CNNVD-202202-1030（CVE-2022-24112）	代码执行	9.8	是	已公开	已公开	未知
	Spring Cloud Gateway	CNNVD-202203-161（CVE-2022-22947）	代码执行	8.0	是	已公开	已公开	已发现
	Splunk	CNNVD-202206-1484（CVE-2022-32158）	代码执行	9.0	否	已公开	未知	未知
	VMware	CNNVD-202205-3716（CVE-2022-22972）	身份认证绕过	9.8	是	已公开	已公开	已发现

Apache APISIX 是一个云原生、高性能、可扩展的微服务 API 网关，在云计算系统中具有广泛的应用，2022 年上半年，该组件曝出了远程代码执行漏洞(CNNVD-202202-1030)，攻击者可通过该漏洞绕过 Apache APISIX 数据平面的 IP 限制，在 Apache APISIX 默认配置下（启用管理 API，使用默认管理密钥且未分配额外的管理端口），攻击者可通过 batch-requests 插件调用 Admin API 执行任意命令。由于 **API 网关在云平台微服务架构中承担着守卫微服务应用入口的重要作用，其出现安全问题将使微服务曝露于风险之中**。

Spring Cloud Gateway 是基于 Spring Framework 和 Spring Boot 构建的 API 网关，它旨在为云原生的微服务架构提供一种简单、有效、统一的 API 路由管理方式。该组件被爆出存在远程代码执行漏洞(CNNVD-202203-161)，当使用 Spring Cloud Gateway 的应用程序启用并公开 Actuator 端点时，远程攻击者可利用该漏洞进行 SpEL 表达式注入攻击，最终在目标服务器上执行任意代码。2022 年 4 月，Securonix 的研究人员在对 Fortinet 发现的 EnemyBot 僵尸网络恶意样本进行分析时发现，该**僵尸网络集成了此漏洞进行网络攻击**。除此之外，还发现 Sysrv-hello 挖矿僵尸网络利用此漏洞攻击用户服务器进行挖矿，严重影响正常用户业务运转。

Splunk Enterprise 是机器数据的引擎软件，广泛应用于云平台中，用于进行数据收集和分析。该软件服务端 9.0 之前的版本存在远程代码执行漏洞(CNNVD-202206-1484)，控制了通用转发器客户端的攻击者，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，将转发器捆绑包通过该服务器部署到其他部署客户端。虽然**该漏洞公开了 POC 代码，但暂未发现有效**

的公开利用代码传播情况。

VMware 是一家传统老牌提供虚拟化解决方案的厂商，其大量产品在企业的云平台、虚拟化系统中广泛部署和使用。2022 年上半年，VMware 被曝存在身份认证绕过漏洞(CNNVD-202205-3716)，影响 VMware Workspace ONE Access Identity Manager 和 vRealize Automation 等多款产品。通过该漏洞，对相关系统 UI 具有网络访问权限的恶意攻击者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。目前**该漏洞的利用代码已经公开，并已经发现在野利用情况。**

（五）边界设备漏洞使网络“大门失守”

路由器、交换机等网络设备是网络连接的枢纽，防火墙、IDS/IPS 等网络安防设备守护着网络的“大门”，一旦控制网络边界设备，其连接的各种终端都将曝露在攻击者面前，一旦突破安防设备，攻击者将如入无人之境，这一切都将造成严重的网络安全危害。2022 年上半年，多款网络边界设备被曝出严重安全漏洞，既有负责网络管理的负载均衡产品，又有防火墙等安全防护设备，还有保障终端安全的防护产品，影响范围覆盖了从互联网到企业内网、从服务器到终端设备。这些漏洞的另一个共同特点就是，因其影响范围广、危害严重，在公开后即被攻击者快速分析，依次研发出具有较好效果的攻击工具进行应用。

表 8 边界设备“明星”漏洞

目标类型	受影响目标	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
网络设备及应用	F5 BIG-IP	CNNVD-202205-2141（CVE-2022-1388）	命令执行	9.8	是	已公开	已公开	已发现
	Zyxel 防火墙	CNNVD-202205-3104（CVE-2022-30525）	命令执行	9.8	是	已公开	已公开	已发现
	Trend Micro Apex Central	CNNVD-202203-2508（CVE-2022-26871）	代码执行	8.6	是	已公开	已公开	已发现

F5 BIG-IP 是美国 F5 公司的一款具备网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台，在全球拥有大量用户。F5 BIG-IP iControl

REST 存在命令执行漏洞 (CNNVD-202205-2141)，该漏洞允许远程未经身份验证的攻击者绕过 iControl REST 服务身份验证访问内部敏感服务，将恶意命令注入到执行的命令行中，从而控制 F5 BIG-IP。由于 F5 BIG-IP 常用于企业级网络中，攻击者借此可以入侵企业网络，进行横向移动、深度渗透等危害行为。该漏洞 POC 及在野利用于 2022 年 5 月 10 日公开，**美国 CISA 于 5 月 18 日专门针对此漏洞发布安全公告，对该漏洞风险进行告警**。

合勤（Zyxel）是一家台湾的网络设备供应商，其网络安全设备在全球具有广泛应用。2022 年 4 月，Zyxel 的 ATP 系列、VPN 系列和 USG FLEX 等系列的防火墙曝出存在远程命令执行漏洞(CNNVD-202205-3104)，远程攻击者可以利用该漏洞在未登录情况下，通过特定 HTTP 接口向防火墙注入恶意命令，攻击者可利用该漏洞反弹 shell、下载恶意模块等，利用方法简单稳定。由于防火墙是边界设备，一旦防火墙遭受威胁，内部脆弱的网络系统也将受到外部攻击者的威胁。Zyxel 于 2022 年 4 月 28 日发布了该漏洞的补丁，一定程度上缓解了危害影响。目前，该漏洞的利用代码已经公开，并已发现在野利用情况。

Trend Micro Apex Central 是一个中央管理控制台，通过策略管理功能，管理员可以进行产品设置并将其部署到受管理的终端。该软件被曝存在任意文件上传漏洞(CNNVD-202203-2508)，远程攻击者可以利用该漏洞上传任意文件到 Trend Micro Apex Central 中，并造成远程代码执行，植入 webshell。该漏洞利用复杂度低，且不需要权限即可上传任意文件到中央服务器，造成远程代码执行并部署 webshell。由于 Trend Micro Apex Central 可以管理受控的终端，一旦失陷将造成极大危害。需要注意的是，目前**已监测到有攻击组织利用该漏洞攻击东南亚某些组织**。

（六）移动终端漏洞威胁个人隐私及数据安全

移动终端作为互联网的另一个重要入口之一，承载了大量的社交、隐私等功能和数据，其安全问题会直接威胁个人隐私及数据安全。移动终端安全漏洞的焦点地位从未改变，尤其是系统层面的高价值漏洞。苹果、Android 作为移动终端的两大主流操作系统，在 2022 年上半年的漏洞情况不容乐观，均曝露出 0day 漏洞及在野利用情况。

表 9 移动终端“明星”漏洞

目标类型	受影响目标	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
移动终端	Apple IOMobileFrameBuffer	CNNVD-202201-2410（CVE-2022-22587）	权限提升	9.8	是	未公开	未公开	已发现
	Apple Webkit	CNNVD-202202-955（CVE-2022-22620）	代码执行	8.8	是	已公开	未公开	已发现
	Google Android	CNNVE-202206-590 (CVE-2022-20130)	代码执行	9.8	否	未知	未知	未知
	Google Pixel	CNNVD-202203-541 (CVE-2021-39793)	权限提升	7.8	否	未知	未知	已发现

2022 年 1 月，美国苹果公司发布安全通告，修复存在于内核中 IOMobileFrameBuffer 权限提升漏洞(CNNVD-202201-2410)，该漏洞存在于 iOS，iPadOS 及 macOS 中，是由于 2021 年 12 月修复的 Apple IOMobileFrameBuffer 权限提升漏洞（CNNVD-202202-955）没有完全修复而产生。通过该漏洞，攻击者可以制作一个恶意应用程序，受害者安装后，攻击者可以在受害者设备以内核权限执行任意代码，从而获取到未授权的受害者设备信息，比如通讯录、照片、视频等等。2022 年 2 月，苹果公司发布安全通告修复存在于 WebKit 浏览器引擎中的 0day 漏洞(CNNVD-202202-955)，这是 Apple 继 CNNVD-202201-2410 后第二次发布 0day 漏洞补丁。Apple 所有型号设备中的浏览器都基于 WebKit 引擎开发，故该漏洞影响 iOS、iPadOS 及 macOS 中所有的浏览器，利用该漏洞需请求恶意链接，成功利用该漏洞可在受害者机器上执行任意代码。**该漏洞最初在 2013 年已完全修复，但在 2016 年代码重构时重新引入**，最终于 2022 年初官方发布通告披露在野利用。该漏洞在野被利用时长暂不清楚，但该漏洞已存在约 5 年时间。

谷歌安卓媒体编码器组件远程代码执行漏洞是由于 tpdec_lib.cpp 中的堆溢出，导致越界写入，未经身份验证的远程攻击者可以利用该漏洞在目标系统上执行任意代码，且无需用户交互。该漏洞**利用方式简单，难度低，场景广泛，通过利用该漏洞攻击者可以控制目标系统**。谷歌 Pixel 本地权限提升漏洞影响搭载着原生的安卓系统谷歌 Pixel/Pixel XL 手机系列。由于 Mali GPU 内核驱动存在越界写入漏洞，攻击者利用该漏洞能够从普通权限提升到 ROOT 权限。谷歌 Pixel 本地权限提升漏洞利用无需用户交互，利用方式简单，难度低，场景广泛，通过利用该漏洞攻击者可以提升用户权限。值得注意的是**该漏洞存在在野利用**。

三、落叶知秋——从漏洞态势看威胁变革

（一）漏洞作为战略资源的地位愈发凸显

漏洞作为网络空间的重要资源，攻防双方对抗的关键核心，漏洞数量持续增长，其受到关注的程度也日益提高。无论从漏洞总量，还是从超高危漏洞占比上来看，2022 年上半年漏洞数量仍然呈持续增长态势，微软、谷歌、Adobe 等全球布局的大厂相关产品仍然是漏洞高发区。2022 年上半年，公开披露的漏洞数量达到近三年来新高。其中排名前十的厂商披露的漏洞数量占到了 27%，这也从侧面反映了大厂产品在当前软件生态中地位的重要性。据知道创宇提供的监测数据显示，2022 年上半年境内外黑客利用漏洞对我国内目标发起了大量攻击，其中利用 Log4j 漏洞的攻击次数就超过 8 千万，占据所有漏洞利用量的榜首，典型漏洞利用攻击以政府机构、教育、IT 行业领域的信息系统为主要目标[31]。

表 10 利用典型漏洞的网络攻击次数

网络攻击重点 重点目标行业	受攻击次数		
	Log4j2 漏洞 （CNNVD-202112-799）	Spring4Shell 漏洞 （CNNVD-202203-2514）	Atlassian Crowd （CNNVD-201905-1031）
政府机构	4,927,131	277,617	213,776
教育	444,048	20,198	13,758
IT 行业	1,154,418	224,876	41,816

漏洞及其管控措施已经成为网络空间博弈的重要方面。2022 年上半年，美国、欧盟等相继出台多项政策、措施，以实施对漏洞的有效管控，一方面在其国内或盟友之间鼓励、激励漏洞的发现及相关资源的共享，另一方面针对特定国家及地区的政府组织和个人，设置了更加严格的条件限制漏洞资源以及相关技术工具的披露、共享等合作。

[31] 知道创宇-创宇安全智脑

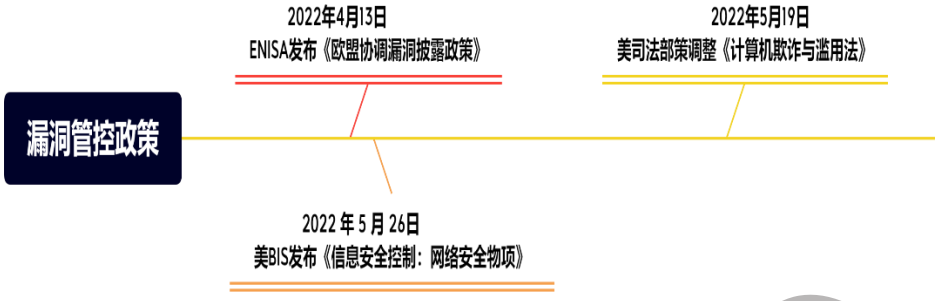


图 8 2022 年上半年发布的主要漏洞管控政策

4 月 13 日，欧洲网络及信息安全局（ENISA）发布《欧盟协调漏洞披露政策》（Coordinated Vulnerability Disclosure Policies in the EU）报告[32]，全面概述欧盟在实施协调漏洞披露（CVD）政策时面临的各种挑战并提出了具体建议，包括修订刑法和网络犯罪指令，为参与漏洞发现的安全研究人员提供法律保护；在为安全研究人员建立任何法律保护之前，定义明确区分“道德黑客”和“黑帽”活动的具体标准；通过国家或欧洲漏洞赏金计划，或通过促进和开展网络安全培训，为安全研究人员制定积极参与 CVD 研究的激励措施等内容。5 月 26 日，美国商务部工业和安全局（BIS）发布《信息安全控制：网络安全物项》[33]，该项规定以维护美国国家安全和反恐为由，新增经授权的网络安全物项出口许可例外，就美国实体与相关国家及地区的政府组织和个人开展网络安全漏洞合作时，以及出口网络安全漏洞检测、修复、披露相关的技术产品时，要事先通过美国商务部的审核，中国亦在受限国家之列。此规定体现了美国在漏洞方面的趋势和动向。5 月 19 日，美国司法部公布一项政策调整，将不再对违反美国联邦黑客法《计算机欺诈与滥用法》（CFAA）[34]的善意安全研究提起诉讼。其所谓的善意安全研究是指仅出于善意测试、调查和/或纠正安全漏洞的目的访问计算机，而此类活动的执行方式旨在避免对个人或公众造成任何伤害，从活动中获得的信息主要用于促进被访问计算机所属的设备、机器或在线服务类别或使用此类设备、机器或在线服务的人的安全性。美国司法部副部长 Lisa O. Monaco 在公告的相关声明中

[32] https://www.enisa.europa.eu/news/enisa-news/coordinated- vulnerability-disclosure-policies-in-the-eu rity-items
[33] https://www.federalregister.gov/documents/2022/05/26/2022-11282/information-security-controls- cybersecu
[34] https://www.justice.gov/opa/press-release/file/1507126/download

表示，“司法部从不打算将善意的计算机安全研究视为应被起诉的罪行。此次公告希望为善意的安全研究人员提供清晰指引，鼓励研究者出于公共利益去根除漏洞。”

（二）各类目标高价值漏洞层出不穷

边界设备在网络中的枢纽作用及“守大门”的重要角色和关键作用，决定了其漏洞在网络攻防中愈发受到关注。通过漏洞突破网络边界设备，能够为攻击者打开通向内网的大门，实现更深层次的攻击渗透。根据统计发现，2021 年上半年期间主流网络设备漏洞数量共计 546 个，达到近三年的峰值，虽然 2022 年上半年数量有所下降，但也有近 300 个之多。近三年主流网络设备漏洞数量统计如图 9 所示。

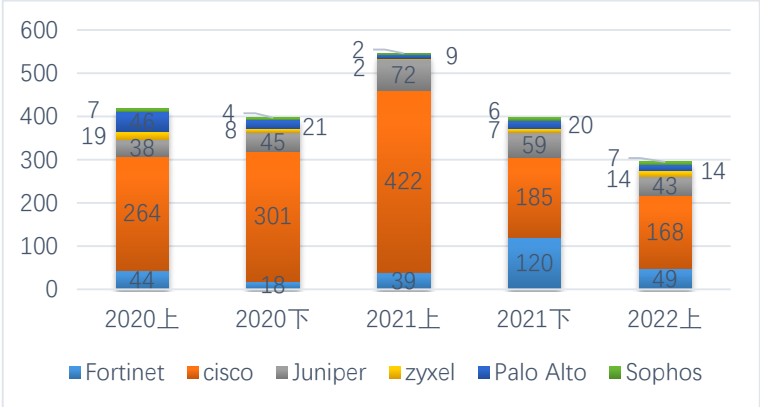


图 9 2020 年-2022 年上半年主流网络设备漏洞统计

根据美国 CISA 已知被利用漏洞统计数据，在 2022 年上半年新增收录的 475 个已知被利用漏洞中，网络边界设备及应用的漏洞数量为 82 个，占比达到了 17%，其中受影响最严重的厂商为美国思科公司。网络设备在野被利用漏洞分布情况如图 10 所示。

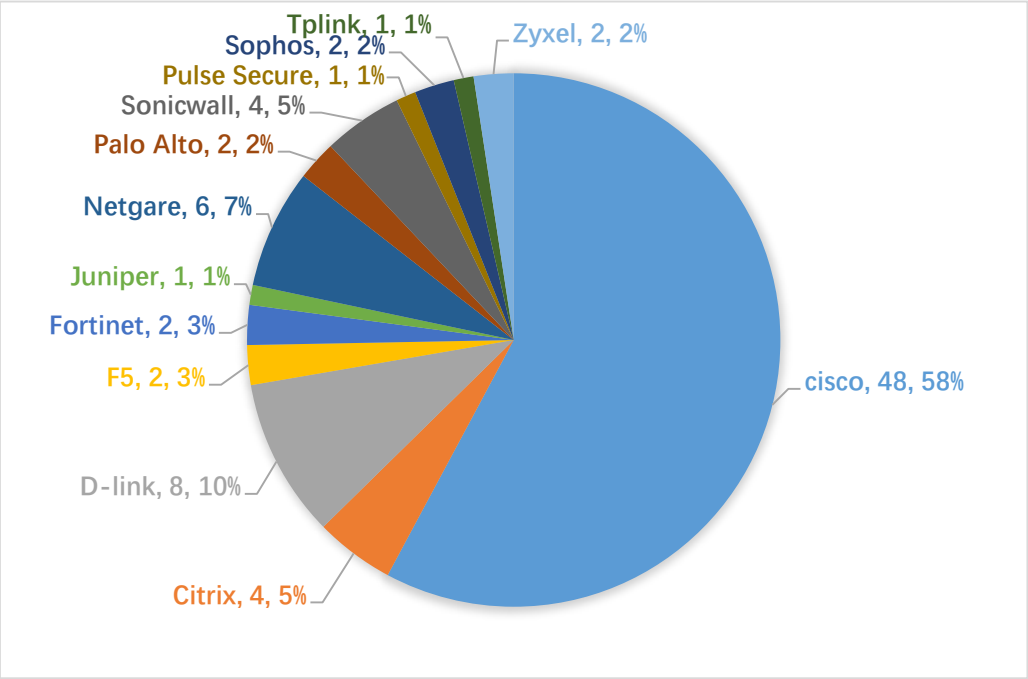


图 10 在野利用漏洞中网络设备相关漏洞的分布

终端作为网络安全战场上的最后一块阵地，始终是攻防双方争夺的焦点。由于此类漏洞能够达到“直捣黄龙”的攻击效果，因此危害仍不容小觑。通过**利用终端应用软件漏洞、操作系统内核漏洞等能够使攻击者直达目标**，获取终端系统、服务器的控制权，进而达到渗透、窃取信息和破坏的目的。2022 年上半年，以办公软件\浏览器软件等消费级软件、Windows\Linux\macOS\Android 等几大操作系统内核等为目标的影响终端安全的漏洞层出不穷。以操作系统为例，2022 年上半年公开披露漏洞共计 665 个，占 2022 年上半年披露漏洞总数的 6%。在四大主流操作系统中，Windows 操作系统漏洞 262 个，占操作系统漏洞数量的 39%；Android 系统漏洞共计 290 个，占比 44%；macOS 漏洞共计 65 个，占比 10%；Linux 内核漏洞 48 个，占比 7%。主要统计情况如图 11 所示。

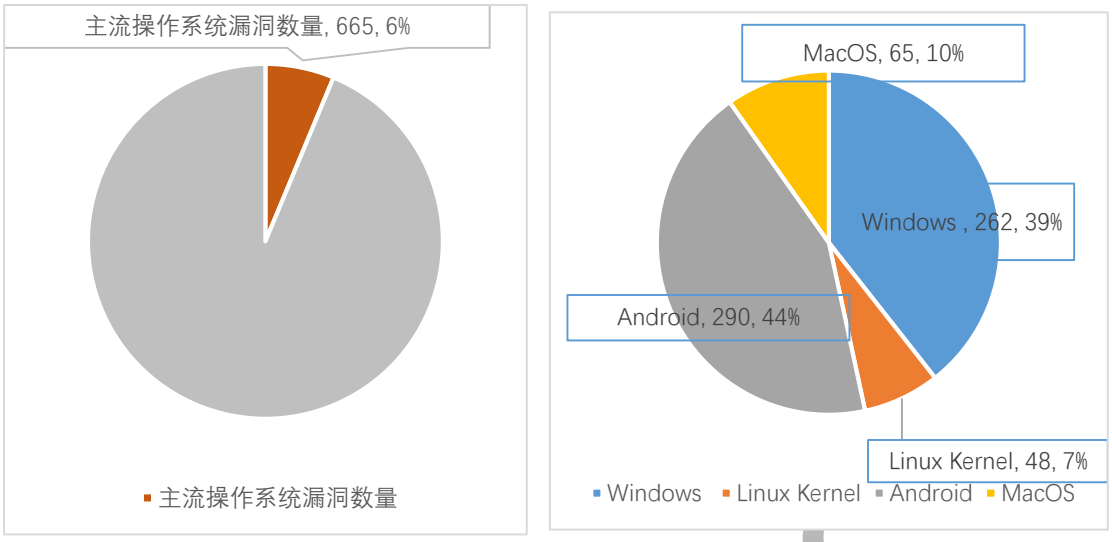


图 11 2022 年上半年操作系统漏洞情况统计

协同办公、远程会议类软件漏洞成为新的关注焦点。受疫情等原因的影响，远程在线办公的需求猛涨，多个远程办公系统、企业 OA 系统、在线会议系统等被爆出高可利用漏洞，攻击者将此类漏洞作为攻击突破口，导致大量企业因此类软件的漏洞受到攻击。在 2022 年 5 月举行的全球最知名的 PWN2Own 2022 黑客大赛，微软 Teams 软件、ZOOM 在线会议软件成为漏洞挖掘和利用的主要目标产品。在大赛首日，参赛队伍就攻破了微软 Teams 软件；在大赛期间，微软 Teams 软件被爆出多个高可利用漏洞，3 只参赛队伍通过不同的漏洞分别构造了针对 Teams 软件的完整攻击链。此外，微软的 MSDT 支持诊断工具的远程代码执行漏洞影响了 OFFICE 全系列产品、Atlassian Confluence 企业协同软件的漏洞影响其服务器安全，国内厂商的向日葵远程控制软件漏洞、钉钉远程办公软件漏洞影响国内大量用户，这几个关键漏洞均发现在野利用的情况，攻击者已经在利用此类漏洞开展网络入侵渗透活动。

供应链安全热度不减，开源软件漏洞首当其冲。在信息技术全球化的背景下，开源软件在各领域得到广泛应用，软件供应链安全热度持续高升。由于开源软件错综复杂的依赖关系，在信息技术领域天然存在的供应链中，放大了传统安全漏洞的危害和影响。

（三）漏洞利用实战化需高度警惕

漏洞在野利用形势严峻，实战化的漏洞利用防不胜防。漏洞的在野利用情况

是体现漏洞真实危害的重要参考，2022 年上半年，漏洞在野利用的形势十分严峻，在野利用漏洞的数量仍呈现整体上升趋势，0day、Nday 高可利用漏洞平分秋色，在现实网络攻击中被普遍使用。需要引起注意的是，一些影响范围广、危害程度高的“骨灰级”历史漏洞仍然受到追捧，甚至在 APT 攻击事件中频繁现身。

据统计，2022 年新增在野被利用漏洞中，近 3 年（CVE 编号为 CVE-2020-XXX 至 CVE-2022-XXX）的漏洞占比为 26%，5 年之前（CVE 编号为 CVE-2016-XXX 以及之前）的漏洞占比达到 39%，如图 12 所示。2022 年新增漏洞中，其中有 43 个被监测到发生在野被利用情况，其中 18 个漏洞最初被发现在野利用时为 0day 状态，占比高达 42%，如图 13 所示。

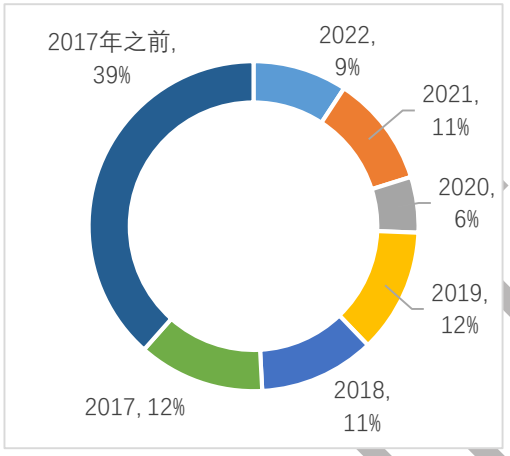


图 12　新增在野被利用漏洞情况

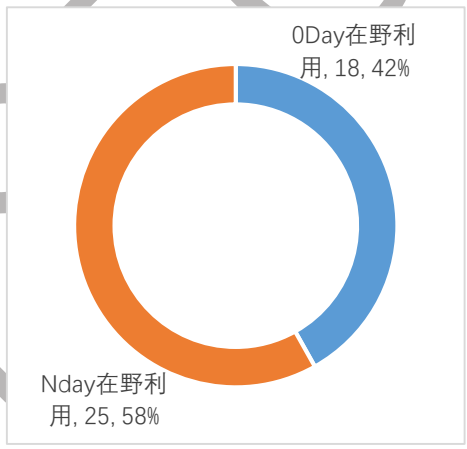
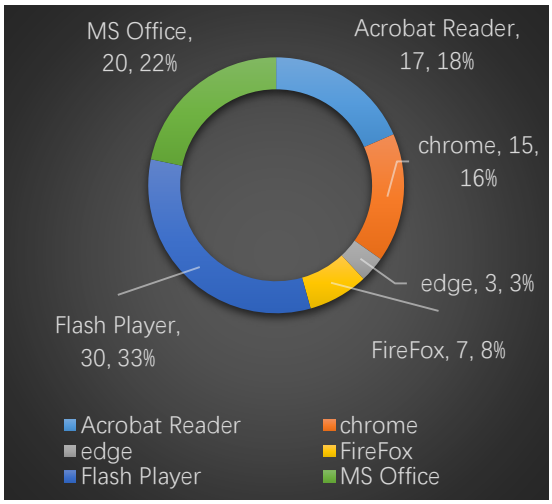


图 13　新增漏洞在野利用情况统计

终端应用软件（如 Acrobat Reader、chrome、edge、FireFox、Flash Player、MS Office 等）被监测到在野被利用漏洞数量共计 92 个，四大主流操作系统被监测到在野被利用漏洞共计 90 个，主要分布情况如图 14 所示



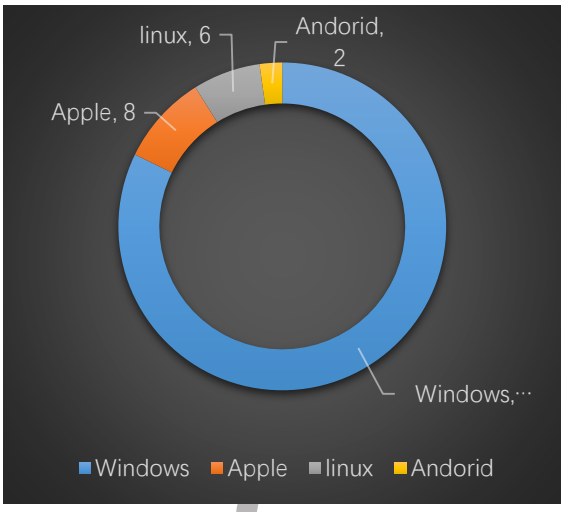


图 14 2022 年上半年终端应用及操作系统 漏洞在野利用情况

在现实网络攻击事件中，大量的在野利用漏洞被发现在 APT 攻击中被使用。据奇安信威胁监测发现，2022 年上半年近 20 个在野利用漏洞被 APT 组织使用，其中 Microsoft Office 漏洞（CNNVD-201711-508）、Microsoft Exchange 漏洞（CNNVD-202107-741、CNNVD-202107-740、CNNVD-202105-543）虽为较为久远的历史漏洞，但由于其影响范围及危害程度，被至少 7 个 APT 组织在攻击中使用。

（四）攻防对抗加剧对漏洞修复提出更高要求

历史漏洞修复后再被突破，漏洞修复从亡羊补牢变成牵萝补屋。在操作系统及软件的漏洞防护措施及缓解机制普遍部署下，网络安全整体防护水平不断在提高。但这种情况并没有阻止漏洞被成功利用，甚至还激发了攻击者探求更高级的漏洞利用手法和技巧，因此厂商对漏洞的修复就变得至关重要。然而，数据显示厂商实际漏洞修复质量不高，很大比例漏洞均是由于厂商没有完全修补造成，漏洞修复从亡羊补牢变成牵萝补屋，导致很大比例已修复漏洞再被利用。

美国谷歌公司发布的报告《2022 年 0day 在野利用——到目前为止》跟踪分析了 2022 年上半年在野被利用的 18 个 0day，报告显示，至少有 9 个 0day 漏洞是先前已修复漏洞的变种，通过更完善、更全面修复和完备测试能够避免这种情况的发生。此外，2022 年在野利用的 0day 漏洞中，有 4 个漏洞为 2021 年在野利用 0day 漏洞的变种，也就是说攻击者在不到 12 个月的时间就突破漏洞的补丁修复方案，又实现了对漏洞的再利用。

表 11 在野利用 0day 漏洞与历史漏洞关联情况

2022 年在野 0day 漏洞	相关联历史漏洞	受影响实体	再现原因
CNNVD-202201-802 (CVE-2022-21882)	CVE-2021-1732	Windows win32k	修补不完善
CNNVD-202201-2410 (CVE-2022-22587)	CVE-2021-30983	iOS IOMobileFrameBuffer	修补不完善
CNNVD-202205-4277 (CVE-2022-30190)	CVE-2021-40444	Windows	——
CNNVD-202203-2278 (CVE-2022-1096)	CVE-2016-5128 CVE-2021-30551 CVE-2022-1232	Chromium Property access interceptors	修补不完善
CNNVD-202204-3442 (CVE-2022-1364)	CVE-2021-21195	Chromium V8	——
CNNVD-202202-955 (CVE-2022-22620)	2013 年修复,2016 年重新引入	WebKit	修补后代码回滚，漏洞重现
CNNVD-202203-541 (CVE-2021-39793)	Linux 不同子系统中存在此漏洞	Google Pixel	——
CNNVD-202206-442 (CVE-2022-26134)	CVE-2021-26084	Atlassian Confluence	——
CNNVD-202205-2846 (CVE-2022-26925)	CVE-2021-36942	Windows PetitPotam	修补后代码回滚，漏洞重现

四、漏洞防范及安全保障对策建议

（一）打造国家级网络安全漏洞综合运筹能力，加强漏洞管控统筹协调，提升漏洞资源共享共治水平

一是强化制度要求。依据中央在网信领域的总体部署和《网络安全法》的基本要求，结合我国国情加强网络安全漏洞管控制度建设，通过网络安全审查等手段方式，加强网络安全漏洞处置与应急响应、风险评估与态势感知体系和能力的建设，提高关键信息基础设施和重要信息系统的安全保障要求，落实厂商及运维相关部门的主体责任要求，科学合理落实《网络产品安全漏洞管理规定》。

二是加强统筹协调。进一步发挥 CNNVD 等国家级漏洞库的信息聚合和服务作用，推动实施多方联动的漏洞资源评估共享机制，提升对网络安全漏洞的管控服务能力和共享共治水平，发挥漏洞资源应用效益的最大化，降低由于漏洞引发的基础性风险。

三是助力网络安全保障。打造以“漏洞”为核心的网络安全漏洞综合运筹及安全保障支撑能力。通过平台建设、机制建设及资源汇聚共享，加大漏洞检测、漏洞防护、漏洞消控等工具研发，实现服务国家网络安全保障的现实需求。

（二）建设国家级漏洞感知与预警机制，提升漏洞发现与处置能力

一是在漏洞发现方面，提升国家级的漏洞自主分析、挖掘和检测能力。一方面通过建设专用的规模化漏洞分析平台，打造专业的漏洞挖掘分析人才队伍，针对重要信息技术产品、系统开展超高危、高可利用 0day 漏洞的分析和挖掘。另一方面，鼓励和支持安全检测机构和社会力量围绕我重要信息系统开展专门的漏洞分析和安全测试，及时掌握高危漏洞的最新动态。通过对未知漏洞的自主发现，一方面支撑对我重要信息系统、关键基础设施的网络安全防护，另一方加强对网络安全漏洞资源的管控，提升漏洞预警、处置能力水平。

二是在漏洞情报采集方面，形成和自主漏洞挖掘的互补，做成漏洞的收集器、过滤器和富化器，提升漏洞情报的感知、获取和预警能力。一方面应建立国家级

的漏洞情报信息感知和采集平台，实现对一手漏洞数据源信息的实时采集和深度挖掘，保证漏洞情报的全面性和及时性；另一方面打造专业的漏洞分析人才队伍，依据完善的流程和专业经验对漏洞的影响面和技术细节进行研判，把真正重要的漏洞过滤出来，保证信息的准确性和预警处置的可靠性；第三，建立全面的多维漏洞信息整合及属性标定，从利用、缓解、防护等角度，富化漏洞信息，为进行漏洞处置提供支撑。

三是在漏洞追踪监测方面，提升系统化漏洞感知能力。一方面以软硬件产品、开源及闭源组件等对象为核心，构建漏洞图谱，开展漏洞追踪及漏洞影响预测。另一方面，开展漏洞实时监测，实现对高隐蔽性、高复杂性网络攻击中漏洞信息的主动识别，尤其是对 APT 攻击中漏洞的准确识别，形成漏洞威胁实时感知能力。

四是在漏洞快速处置及应用方面，提升漏洞消控及防御保障能力，打赢漏洞攻防时间战。目前，从漏洞信息公开到实际利用攻击出现的间隔期越来越短，大多数时候攻防双方是在时间战中角逐。研究典型漏洞利用攻击的快速反应技术和相关机制，结合国家网络安全保障需求，形成有效的网络安全漏洞主动防御能力。

（三）积极推进 ICT 供应链安全治理，完善符合我国情的开源生态

一是在法律法规及标准规范方面，相关部门应根据我国 ICT 供应链的现状有针对性地制定供应链安全治理相关规定，同时配套制定形成体系化的 ICT 供应链安全标准，从法律法规、标准体系等方面形成系统化的治理措施，为开展 ICT 供应链安全治理提供依据。

二是在风险管控方面，监管部门应尽快指导建立关键基础设施的 ICT 供应链台账，理清家底，查摆问题，预判风险。同时，ICT 供应链的供给侧、需求方均需加强供应链安全管控，尤其是涉及关键技术设施运营的供需方，需开展 ICT 供应链安全审查、评估和威胁监测，提升供应链韧性。

三是在技术层面，通过技术手段开展 ICT 供应链安全检测，对软件成分、来源及安全漏洞进行准备分析和定位，针对 ICT 产品构建形成物料清单和构成图谱，为关键 ICT 产品进行“精准画像”，一方面提前预判风险，另一方面在威胁来临时能够快速处置。建立国家级供应链安全检测及风险分析平台，提升 ICT 供应链安全检测的广度和深度，及时对供应链安全风险进行预警。

附件 **2022 年上半年明星漏洞回顾**

2022 年上半年，针对操作系统、开源组件、协同办公软件、云原生及虚拟化软件、网络设备、移动平台等目标对象，均披露了多个具有较大影响的漏洞，并在实际网络攻击中产生了较大的现实威胁。本报告对其中的 29 个明星关键漏洞进行了分析，主要情况如下。

表 2022 年上半年关键漏洞信息

目标类型	受影响目标	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
操作系统及服务器	Windows Remote Desktop	CNNVD-202203-691（CVE-2022-21990）	代码执行	8.8	是	已公开	未知	未知
	Windows AD域	CNNVD-202205-2850（CVE-2022-26923）	权限提升	8.8	是	已公开	已公开	未知
	Exchange Server	CNNVD-202201-734（CVE-2022-21846）	代码执行	9.0	否	未知	未知	未知
		CNNVD-202201-730（CVE-2022-21855）	代码执行	9.0	否	未知	未知	未知
		CNNVD-202201-731（CVE-2022-21969）	代码执行	9.0	否	未知	未知	未知
	HTTP 协议栈	CNNVD-202201-779（ CVE-2022-21907）	代码执行	9.8	是	已公开	未知	未知
	Windows RPC	CNNVD-202204-3019 (CVE-2022-26809)	代码执行	9.8	是	未知	未知	未知
	Windows Network File System	CNNVD-202205-2781（ CVE-2022-26937）	代码执行	9.8	是	已公开	未知	未知
	Linux DirtyPipe	CNNVD-202203-522（CVE-2022-0847）	权限提升	7.8	是	已公开	已公开	未知
	Linux Polkit	CNNVD-202201-2343（CVE-2021-4034）	权限提升	7.8	是	已公开	已公开	未知
开源组件	Apache Struts2	CNNVD-202204-3223（CVE-2021-31805）	代码执行	9.8	是	已公开	已公开	未知
	Zabbix	CNNVD-202201-2514（CVE-2021-46088）	代码执行	7.2	是	已公开	已公开	未知
协同办公软件	Windows MSDT	CNNVD-202205-4277（CVE-2022-30190）	代码执行	7.8	是	已公开	已公开	已发现
	MS SharePoint Server	CNNVD-202202-580（CVE-2022-22005）	代码执行	9.0	否	未知	未知	未知
		CNNVD-202205-2730（CVE-2022-29108）	代码执行	9.0	否	未知	未知	未知
	Atlassian Confluence	CNNVD-202206-442（CVE-2022-26134）	代码执行	9.8	是	已公开	已公开	已发现
	向日葵	CNVD-2022-10270	代码执行	9.8	是	已公开	未知	已发现
	钉钉	NA	代码执行	8.8	是	已公开	未知	已发现
云原生及虚拟化	Apache APISIX	CNNVD-202202-1030（CVE-2022-24112）	代码执行	9.8	是	已公开	已公开	未知
	Spring	CNNVD-202203-161	代码执行	8.0	是	已公开	已公开	已发现

	Cloud Gateway	（CVE-2022-22947）						
	Splunk	CNNVD-202206-1484（CVE-2022-32158）	代码执行	9.0	是	已公开	未知	未知
	VMware	CNNVD-202205-3716（CVE-2022-22972）	身份认证绕过	9.8	是	已公开	已公开	已发现
网络设备及应用	F5 BIG-IP	CNNVD-202205-2141（CVE-2022-1388）	命令执行	9.8	是	已公开	已公开	未知
	Zyxel 防火墙	CNNVD-202205-3104（CVE-2022-30525）	命令执行	9.8	是	已公开	已公开	已发现
	Trend Micro Apex Central	CNNVD-202203-2508（CVE-2022-26871）	代码执行	8.6	是	已公开	已公开	已发现
移动平台	Apple IOMobileFrameBuffer	CNNVD-202201-2410（CVE-2022-22587）	权限提升	9.8	是	未公开	未公开	已发现
	Apple Webkit	CNNVD-202202-955（CVE-2022-22620）	代码执行	8.8	是	已公开	未公开	已发现
	Google Android	CNNVE-202206-590 (CVE-2022-20130)	代码执行	9.8	否	未知	未知	未知
	Google Pixel	CNNVD-202203-541 (CVE-2021-39793)	权限提升	7.8	否	未知	未知	已发现

1 操作系统及服务器关键漏洞回顾

1.1 Remote Desktop Client 远程代码执行漏洞

漏洞简介：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。Remote Desktop Client 存在远程代码执行漏洞(CNNVD-202203-691)，在微软发布安全通告前，此漏洞 PoC 已在互联网公开。

危害描述：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。

1.2 Windows AD 域权限提升漏洞

漏洞简介：Active Directory 域服务(AD DS)是 Active Directory 中的核心组件，它存储和管理连接到网络的用户、设备和服务信息，使用户能够对网络上的资源进行身份验证和访问，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。

Active Directory 域权限提升漏洞(CNNVD-202205-2850)允许攻击者在开启了证书认证的域中，仅拥有普通用户权限即可提升到域控权限，该漏洞于 2022 年 5 月 10 日由国外安全研究员公开细节及利用 PoC，攻击者可以修改拥有的账户创建的机器账户的 dNSHostName 属性，之后使用这个机器账户申请认证机器证书即可得到域控权限的认证证书，使用该证书进行身份验证，成功利用该漏洞的攻击者可以获取到域控权限，从而完全控制域，微软于 5 月微软补丁日发布了该漏洞补丁。

危害描述：通过利用该漏洞攻击者可以获取到域内域控的权限，利用域控权限可以完全控制接入域内的服务器、电脑、打印机等，对企业网络造成威胁。

1.3 Microsoft Exchange Server 远程代码执行漏洞

漏洞简介：Microsoft Exchange Server 在全球拥有大量用户，是企业和学术机构最常用的电子邮件服务器。其运行在 Windows Server 上，使用 Active Directory 来存储和共享目录信息。作为最常用的电子邮件解决方案，Exchange Server 一直都是黑客的首要目标。如果黑客发起攻击，可能导致用户敏感数据泄露，给企业和用户带来重大损失。

2022 年 1 月，Microsoft Exchange Server 公开了几个远程执行代码漏洞，包括：CNNVD-202201-734、CNNVD-202201-730 以及 CNNVD-202201-731。其中，CNNVD-202201-734 被微软标记为紧急漏洞，CNNVD-202201-730 和 CNNVD-202201-731 风险等级为重要。

危害描述：由于没有对用户提供的输入进行充分验证，相邻网络中经过身份验证的攻击者可以向目标 Exchange 服务器发送特制数据来利用此漏洞，从而在目标系统上执行任意代码，利用该漏洞无需用户交互。

1.4 HTTP 协议栈远程代码执行漏洞

漏洞简介：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（CNNVD-202201-779），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。

危害描述：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。

1.5 Windows Network File System 远程代码执行漏洞

漏洞简介：网络文件系统 (NFS) 是一种用于分布式文件共享的网络协议，它定义了跨网络从存储设备存储和检索文件的方式。使用 NFS 协议可以在 Windows 计算机和其他非 Windows 操作系统（如 Linux 或 UNIX）之间传输文件。

危害描述：Windows Network File System 存在远程代码执行漏洞，漏洞编号为 CNNVD-202205-2781。由于 Windows Network File System 对用户提供的输入的验证不充分。远程攻击者可通过向 NFS 服务器发送特制数据包来利用此漏洞，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。

1.6 Windows RPC Runtime 远程代码执行漏洞

漏洞简介：Windows RPC 运行时系统是用于处理 RPC 机制网络通信的例程和服务库。在 RPC 调用过程中，客户端和服务器端运行时系统用于处理绑定、建立通信、传递调用数据以及处理通信错误的场景。RPC Runtime 存在远程代码执行漏洞，由于该漏洞主要是 RPC Runtime 在处理网络数据的过程中缺乏校验，存在整数溢出问题，可允许攻击者绕过后面的判断逻辑进行越界读写。

危害描述：Windows RPC Runtime 存在远程代码执行漏洞，攻击者可通过向目标系统发送特制的 RPC 数据包来利用此漏洞，这可能会允许攻击者在服务器端以与 RPC 服务相同的权限执行任意代码。尽管此漏洞评分较高，但在默认配置下难以触发，还需依赖于特定的环境，并且从越界读写到代码执行的过程难以实现。

1.7 Linux DirtyPipe 内核本地权限提升漏洞

漏洞简介：管道是进程之间的单向数据流，一个进程写入管道的所有数据都由内核路由到另一个进程，另一个进程可以从管道中读取数据。Linux 内核存在未初始化变量漏洞，在调用 copy_page_to_iter_pipe 函数的时候，没有初始化 flags 变量，导致后面延用之前的页面缓存时会使用之前设置的 flags 变量。攻击者可以利用该漏洞覆盖之前的页面内存，从而实现本地权限提升。

危害描述：Linux 内核存在本地权限提升漏洞(CNNVD-202203-522)EXP 已公开，且利用难度低。当攻击者获取到 Linux 的普通权限用户时，可以利用该漏洞进行本地权限提升，获取到 root 权限。

1.8 Linux Polkit 本地权限提升漏洞

漏洞简介：Polkit 是一个用于在类 Unix 操作系统中控制系统范围权限的组件，它为非特权进程与特权进程提供了一种通信方式。Polkit 中的 pkexec 应用程序旨在允许非特权用户根据预定义的策略以特权用户身份运行命令。Pkexec 不正确的处理

argc，当 argc==0 时存在 OOB，可以越界访问到环境变量。攻击者可以控制环境变量，导致本地权限提升。

危害描述：Linux Polkit 存在本地权限提升漏洞(CNNVD-202201-2343)，该漏洞代码已引入 13 年，影响几乎所有的主流 Linux 操作系统。该漏洞 EXP 已公开，利用难度低。当攻击者获取到 Linux 的普通权限用户时，可以利用该漏洞进行本地权限提升，获取到 root 权限。

2 开源组件关键漏洞回顾

2.1 Apache Struts2 远程代码执行漏洞

漏洞简介：Apache Struts 是最早的基于 MVC 模式的轻量级 Web 框架，它能够合理划分代码结构，并包含验证框架、国际化框架等多种实用工具框架。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 曝出很多远程代码执行漏洞，而 CNNVD-202204-3223（S2-62）是其前一个漏洞 S2-61 的绕过，时隔一年左右的时间，同样是 OGNL 表达式注入漏洞。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，从而执行恶意代码。

危害描述：Apache Struts2 历史漏洞几乎均为 OGNL 表达式注入导致远程代码执行漏洞，攻击者发送特定请求则可执行代码。同时 Apache Struts 官方发布该漏洞通告时表明不再接收由未经验证的用户输入引起的 OGNL 表达式二次解析问题。这给我们以警醒，开发人员应严格控制用户输入。

2.2 Zabbix 远程代码执行漏洞

漏洞简介：Zabbix 是一个基于 WEB 界面的提供分布式系统监视以及网络监视功能的企业级的开源解决方案。Zabbix 能监视各种网络参数，保证服务器系统的安全运营；并提供灵活的通知机制以让系统管理员快速定位/解决存在的各种问题。

Zabbix 存在远程代码执行漏洞 (CNNVD-202201-2514) 。任何具有“Zabbix Admin”角色的用户都可以在对应 Server 服务器上运行自定义 shell 脚本。攻击者可通过该漏洞在 Agent 中执行任意代码并获取权限。

危害描述：该漏洞触发需要”Zabbix Admin”权限，当 Agent 配置

EnableRemoteCommand=1 或`AllowKey=system.run[*]`时(该场景较为常见)，通过在 Server 端添加 item key，创建 action 并在 command 处配置恶意代码、创建 trigger 触发 action 执行恶意代码，该漏洞虽然利用难度较高，但若管理员身份凭证泄漏，那么将影响企业中所有部署 Zabbix Agent 的服务器，影响面极其广泛。

3 协同办公软件关键漏洞回顾

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

漏洞简介：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。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。

危害描述：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相应缓解措施，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。

3.2 Microsoft SharePoint Server 远程执行代码漏洞

漏洞简介：Microsoft SharePoint Server 是由微软提供的用以提供基本的门户网站和企业内网功能的软件。超过 200,000 个组织和 1.9 亿人将 SharePoint 用于 Intranet、团队网站和内容管理。2022 年上半年，Microsoft SharePoint Server 公开了多个远程执行代码漏洞，其中，CNNVD-202202-580 和 CNNVD-202205-2730 被微软标记为“Exploitation More Likely”。

危害描述：这些漏洞允许经过身份验证的用户在目标服务器上以 SharePoint Web

服务帐户权限执行任意代码。攻击者需要拥有创建页面的权限才能利用此漏洞，默认情况下，经过身份验证的用户能够创建自己的站点，在这种情况下，用户将拥有所有必要的权限。

3.3 Atlassian Confluence 远程代码执行漏洞

漏洞简介：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 及 Confluence Data Center 中曝出严重的远程代码执行漏洞。未经身份验证的远程攻击者通过注入 OGNL 表达式从而执行任意代码，利用极其简单。该漏洞在 6 月 2 日发布时尚未修复，影响所有 Confluence Server 及 Data Center 版本，且已发现在野利用。截至 6 月 3 日，官方发布的补丁和临时解决方案均可用。

危害描述：Atlassian Confluence 在去年 8 月份曝出一 OGNL 表达式注入漏洞，漏洞评级为严重。同样是由于 OGNL 表达式注入引起，今年的漏洞，任意用户仅通过发送一条 HTTP GET 请求即可在目标服务器上 RCE，获取服务器权限。由于漏洞利用难度极低，之后披露出多起攻击事件均利用此漏洞进行攻击。

3.4 向日葵远程代码执行漏洞

漏洞简介：向日葵远程控制软件是一款免费的集远程控制电脑手机、远程桌面连接、远程开机、远程管理、支持内网穿透的一体化远程控制管理工具软件。随着远程办公人数的增加，越来越多的员工通过该软件远程操控公司中的电脑，同时，也带来了许多安全问题。2022 年 2 月，向日葵远程控制软件 Windows 版本远程命令执行漏洞公开时已发现在野利用，远程攻击者可以在未授权情况下获取到对应机器的 CID，然后可通过该 CID 构造特殊请求在目标机器上执行任意命令。

危害描述：由于部分企业的安全意识不足，将向日葵的接口主动曝露在公网，在漏洞公开后，很多企业受到了攻击，包括挖矿、勒索、僵尸网络等，且漏洞影响的对应版本不能通过自动升级的方式进行软件升级，导致的后果是给了不法分子更充足的时间进行恶意攻击，从而使企业遭受更大的损失。

3.5 钉钉远程代码执行漏洞

漏洞简介：钉钉（DingTalk）是阿里巴巴集团专为中小企业打造的沟通和协同的

多端平台。钉钉因中小企业而生，帮助中小企业通过系统化的解决方案，全方位提升中小企业沟通和协同效率，自疫情爆发以来，钉钉在远程办公、线上授课等方面都有很多的应用。2022 年 2 月，钉钉远程代码执行漏洞公开时已发现在野利用，攻击者通过将恶意链接发送至受害者，诱使受害者点击该链接，钉钉即会获取恶意链接指向的网页内容并用内置浏览器渲染，从而触发漏洞，在受害者电脑上远程执行代码。

危害描述：通过该漏洞，攻击者可将受害者的机器当作跳板机，用来攻击企业内网，从而获取企业内部数据，使企业遭受不必要的损失。

4 云原生及虚拟化关键漏洞回顾

4.1 Apache APISIX 远程代码执行漏洞

漏洞简介：Apache APISIX 是一个云原生、高性能、可扩展的微服务 API 网关，同时提供了多平台解决方案，不但支持裸机运行，也支持集成在 Kubernetes 中。Apache APISIX 中默认启用的 batch-requests 插件存在重写 X-REAL-IP 标头的风险，攻击者可通过该漏洞绕过 Apache APISIX 数据平面的 IP 限制。在 Apache APISIX 默认配置下（启用管理 API，使用默认管理密钥且未分配额外的管理端口），攻击者可通过 batch-requests 插件调用 Admin API 执行任意命令。

危害描述：Apache APISIX 远程代码执行漏洞源于 X-REAL-IP 头限制绕过，最终在默认配置下导致服务端执行任意代码。看似影响有限的漏洞，组合系统中其他弱功能点造成的影响却不在预期范围内，开发人员应重视系统中每一个弱点进行加固。

4.2 Spring Cloud Gateway 远程代码执行漏洞

漏洞简介：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 端点时，远程攻击者可利用该漏洞进行 SpEL 表达式注入攻击，最终在目标服务器上执行任意代码。

危害描述：EnemyBot 是一个基于多个恶意软件代码的僵尸网络，它通过迅速增加对最近披露的网络服务器、内容管理系统、物联网和 Android 设备的关键漏洞的利用来扩大其影响范围。该僵尸网络于 3 月由 Securonix 的研究人员首次发现，在 4 份对 Fortinet 的新样本进行分析时，发现 EnemyBot 已经集成了十几种处理器架构的漏

洞，其中就包含 Spring Cloud Gateway 远程代码执行漏洞(CNNVD-202203-161) 。除此之外，Sysrv-hello 挖矿僵尸网络利用此漏洞攻击用户服务器进行挖矿，严重影响正常用户业务运转。

4.3 VMware 多个产品身份认证绕过漏洞

漏洞简介：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。

危害描述：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，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。

4.4 Splunk Enterprise 远程代码执行漏洞

漏洞简介：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。

危害描述：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。

5 网络设备及应用关键漏洞回顾

5.1 F5 BIG-IP 命令执行漏洞

漏洞简介：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，这允许用户与 F5 设备之间进行轻量级、快速的交互。

F5 BIG-IP iControl REST 存在命令执行漏洞（CNNVD-202205-2141）。该漏洞允许远程未经身份验证的攻击者绕过 iControl REST 服务身份验证访问内部敏感服务，通过命令注入将恶意命令注入到执行的命令行中，进而执行任意命令，该漏洞 PoC 及在野利用事件于 2022 年 5 月 10 日公开。

危害描述：未经身份验证的远程攻击者可以向 F5 BIG-IP iControl 注入操作系统命令，在 F5 BIG-IP iControl 上执行恶意命令，从而控制 F5 BIG-IP，而 F5 BIG-IP 常用于企业级网络中，攻击者借此可以入侵企业网络，进行横向移动、深度渗透等危害行为。

5.2 Zyxel 防火墙远程命令执行漏洞

漏洞简介：在 zyxel 的 ATP 系列、VPN 系列和 USG FLEX 等系列的防火墙通常用于小型公司和机构中，提供 VPN 解决方案、SSL 检查、Web 过滤、入侵保护和电子邮件安全等功能。在这些系列的防火墙中存在命令注入漏洞，远程攻击者可以利用该漏洞在未登录情况下向防火墙注入恶意命令，通过 nobody 权限执行恶意命令。攻击者向 HTTP 接口内的 mtu 参数通过 shell 元字符注入恶意命令，从而造成远程命令执行。

危害描述：攻击者在无需登录情况下即可利用漏洞在受影响的防火墙上远程执行命令，可以利用该漏洞反弹 shell、下载恶意模块等，由于防火墙是边界设备，一旦防火墙遭受威胁，内部脆弱的网络系统也将受到外部攻击者的威胁，利用该漏洞仅需向特定 HTTP 接口注入命令即可，利用简单稳定，极大方便了攻击者利用。Zyxel 于 2022 年 4 月 28 日发布了该漏洞的补丁，一定程度上缓解了此漏洞利用。

5.3 Trend Micro Apex Central 远程代码执行漏洞

漏洞简介：Trend Micro Apex Central 是一个中央管理控制台，透过策略管理功能，管理员可以进行产品设置并将其部署到受管理的终端。在 Trend Micro Apex Central 中存在任意文件上传漏洞,远程攻击者可以利用该漏洞上传任意文件到 Trend Micro Apex Central 中，并造成远程代码执行，植入 webshell。需要注意的是目前已监测到有攻击组织利用该漏洞攻击东南亚某些组织。

危害描述：该漏洞利用复杂度低,且不需要权限即可上传任意文件到 Trend Micro Apex Central 造成远程代码执行并部署 webshell 到服务器，而 Trend Micro Apex Central 可以管理受控的终端，一旦失陷将造成极大危害。

6 移动平台关键漏洞回顾

6.1 Apple IOMobileFrameBuffer 权限提升漏洞

漏洞简介：Apple 在 1 月底发布安全通告修复存在于内核中的 0day 漏洞，该漏洞存在于 iOS，iPadOS 及 macOS 中，该漏洞是由于 Apple 十二月修复的 Apple IOMobileFrameBuffer 权限提升漏洞没有完全修复。

危害描述：攻击者可以制作一个恶意应用程序，受害者安装后，攻击者可以在受害者设备以内核权限执行任意代码，从而获取到未授权的受害者设备信息，比如通讯录，照片，视频等等。

6.2 Apple WebKit 释放后重用漏洞

漏洞简介：Apple 在 2 月份发布通告修复一存在于 WebKit 浏览器引擎中的 0day 漏洞,这是 Apple 继 CVE-2022-22587、CVE-2022-22594 后第二次发布 0day 漏洞补丁。Apple 系统中所有浏览器都基于 WebKit 浏览器引擎开发，故 Apple WebKit 释放后重用漏洞影响 iOS、iPadOS 及 macOS 中所有的浏览器，利用该漏洞需请求恶意链接，成功利用此漏洞可能在受害者机器上执行任意代码。

危害描述：Apple WebKit 释放后重用漏洞最初在 2013 年已完全修复，但在 2016 年代码重构时重新引入该漏洞，最终于今年初官方发布通告披露在野利用。我们虽然不知道此漏洞在野外被利用的时长，但从 2016 年底到 2022 年初该漏洞已存在约 5 年时间。

6.3 Google Android 远程代码执行漏洞

漏洞简介：Google Android 是 Google 以 Apache 免费开放源代码许可证的授权方式开源的基于 Linux 内核的移动操作系统，主要使用于移动设备，如智能手机和平板电脑。该漏洞存在于媒体编码器组件中，在 tpdec_lib.cpp 中由于堆溢出，可能导致越界写入，未经身份验证的远程攻击者可以利用该漏洞在目标系统上执行任意代码，且无需用户交互。

危害描述：Google Android 远程代码执行漏洞利用无需用户交互，且可远程利用，利用方式简单，难度低，场景广泛，通过利用该漏洞攻击者可以控制目标系统。

6.4 Google Pixel 本地权限提升漏洞

漏洞简介：Google Pixel/Pixel XL 是 Google 推出的 Android 手机系列，搭载着原生的安卓系统。在 Mali GPU 内核驱动里面，存在越界写入漏洞，拥有普通权限的攻击者可以利用该漏洞在目标系统上提升权限到 ROOT。

危害描述：Google Pixel 本地权限提升漏洞的利用无需用户交互，利用方式简单，难度低，场景广泛，通过利用该漏洞攻击者可以提升用户权限。值得注意的是该漏洞存在在野利用。

联系方式：010-82341405