360数字安全
数字安全的领导者

2024年度
网络安全漏洞分析报告

360数字安全集团·漏洞情报服务

2025年1月

前言

在数字化进程不断加快的2024年，网络安全愈发成为全球关注的焦点。

随着信息技术的广泛应用，网络攻击的手段和技术层面越来越复杂，这不仅挑战着企业和个人的安全防线，也对社会的安全管理和意识提出了更高的要求。

我们的专家团队对2024年爆发的漏洞情况进行了深入分析，全面剖析了24年网络安全漏洞发展趋势，编写了这份《2024年度网络安全漏洞分析报告》。

报告通过综合分析2024年漏洞的整体态势，对漏洞数量、类型及严重程度进行了细致研究，并揭示了不同行业中的漏洞分布及其差异原因。我们精选了多起典型的漏洞案例，涵盖了从软件平台到操作系统的广泛范围，深入解析这些漏洞的技术细节和潜在影响。

除此之外，报告还拓展了一系列影响深远的全球网络安全热点新闻事件，包括大规模数据泄露、复杂网络攻击以及供应链软件安全问题，全面揭示了全球网络安全所面临的严峻挑战与复杂形势。同时，我们梳理了2024年全球各国在网络安全领域出台或调整的法规动态，帮助企业、机构及相关从业者深入理解最新政策要求，提升合规能力，以更好地应对快速变化的网络安全环境。

我们希望这份报告不仅是对过去一年网络安全态势的总结，更成为未来行动的指南。期待它能为企业、机构及专业人士提供有价值的洞察，助力其在数字化转型的道路上更好地构建安全防线，确保稳健前行。

目录

一、 漏洞云专家点评

本章节是漏洞云专家对 2024 年爆发的漏洞数据以及全球的网络安全现状的点评与思考。

1. 漏洞数量激增对全球网络安全体系构成严峻挑战

a) 年度漏洞数量显著增加，持续威胁网络安全

2024 年，漏洞总数达到 44,957 个，相较 2023 年增长超过 50%，创下历史新高。这一趋势可能反映了漏洞挖掘技术的进步、全球信息安全意识的提升，以及更多软件系统被纳入安全审查。尤其是在 10 月份，漏洞数大幅增加至 14,637 个。这一激增可能是由于多个因素的影响，如大量漏洞在经过长时间的挖掘和处理后集中披露，或某些重要软件更新导致的漏洞被广泛发现和修复。

b) OA 系统漏洞依然是攻防演练中的主要杀器

2024 年，360 漏洞情报发布了超 800 条需高度关注且需要快速修复的漏洞情报，其中 600 条易被利用，300 余条为高危漏洞。在年度攻防演练中，360 漏洞情报捕获 80,702 条攻击样本，发布漏洞预警 180 余条，其中高危及严重级别漏洞占比超过 98%。SQL 注入以 37%的利用率位居首位，OA 系统成为攻击重灾区，ERP 等核心业务系统紧随其后。通过订阅专业漏洞情报服务，企业可精准定位关键风险并前置修复，结合主动防御策略，可有效降低 80%以上的攻击威胁。

c) 高频漏洞类型暴露常见技术缺陷

跨站点脚本攻击（XSS，7,179 个）和 SQL 注入（3,293 个）等经典漏洞依然高居前列，说明许多系统在基本安全设计与开发实践中仍存在顽疾。此外，“权限管理不当”和“访问控制不当”等类型漏洞高发，表明开发者在开发逻辑上的安全思考还有待提高。应加强开发者培训、代码审查和增加产品发布前的人工渗透测试环节是解决这些问题的关键。

d) 跨行业漏洞高发，关键领域安全亟待增强

360 独家研发的行业分类标准实现了对全量漏洞数据的标准化分析。从行业分布来看，通用行业漏洞占比接近 90%，表明跨行业的通用软件和平台是主要薄弱点；而教育、金融和医疗卫生等关键领域也暴露了大批漏洞，凸显了行业特定应用的脆弱性。在产品层面，Linux Kernel（4,531 个）和 Windows 系列产品漏洞占比较高，可能是由于其广泛使用和系统的复杂性导致的。

2. 供应链攻击与数据泄露成为网络安全的主要威胁

a) 供应链攻击频发，加剧系统脆弱性

Red Hat 与 CISA 发现的供应链漏洞、CocoaPods 依赖管理器的多个安全缺陷等，凸显了软件供应链的安全隐患。供应链攻击往往影响范围广、缓解难度大，攻击者利用第三方库、工具或服务的弱点来传播恶意代码，进而攻击下游使用者。加强对供应链的全面审计和监控是防范此类攻击的必要手段。

b) 数据泄露事件规模空前，影响深远

2024 年发生了多起重大数据泄露事件，如 AT&T 的 1.09 亿用户信息泄露和 Change Healthcare 涉及 1 亿人的数据外泄。这些事件不仅对受害者造成身份窃取、财务欺诈等直接风险，还可能对全球信任体系带来长期损害。企业需强化数据加密和存储策略，防止信息泄露问题出现。

c) 勒索攻击与数据窃取手段多样化

BlackCat 组织窃取了 Change Healthcare 的 6TB 数据、CDK Global 因连续遭受勒索攻击关闭系统等案例表明，勒索攻击和数据窃取呈现出更高的精准性和多样性。攻击者通常利用社会工程、系统漏洞等展开勒索行动。企业需要通过外采威胁情报能力、漏洞情报能力扩充自身威胁信息的获取渠道，补齐信息短板，并增强内部人员的信息安全培训来缓解这些威

胁。

3. 全球网络安全法规与政策框架日益完善

a) 数据保护与合规标准加速出台

2024 年我国发布了《网络数据安全管理条例》和《促进和规范数据跨境流动规定》，以及 GB/T 43697-2024 数据分类分级国家标准，均反映了数据保护领域的立法和标准化步伐加快。这些法规将有效规范数据处理活动、保障个人信息安全，同时为国际数据传输和跨境合作提供明确指引。

b) AI 与新兴技术的治理成为重点

联合国通过的人工智能全球决议、欧盟的《人工智能法案》，以及中国《人工智能生成合成内容标识办法（征求意见稿）》的发布，体现了全球各国对 AI 技术潜在风险的高度关注。这些努力既促进了 AI 的创新应用，也试图防止技术被滥用，同时推动公平、安全的使用环境。

c) 鼓励白帽黑客与中小企业网络安全参与

德国的白帽黑客立法、美国的小微企业网络安全税收抵免计划等，体现了对网络安全多样化参与的重视。通过合法化白帽黑客行动以及为中小企业提供支持，这些政策有助于弥合网络安全领域的能力差距，构建更广泛的协作生态系统。

4. 全球化威胁与区域化事件并存，凸显网络安全国际合作的重要性

a) 大型事件频发，影响关键基础设施

法国奥运期间遭遇 140 多起网络攻击、西雅图港 IT 系统瘫痪、日本航空公司网络攻击导致航班延误等事件表明，关键基础设施面临着愈发复杂的网络威胁。

b) 执法行动与国际合作成效初显

欧洲刑警组织协调的“PowerOFF”行动成功拆除了 15 个国家的 DDoS 攻击平台，而联合国通过的网络犯罪公约为各国协调执法提供了框架。这些行动表明，国际合作在应对跨国网络犯罪和保护全球数字生态方面不可或缺。

二、 漏洞整体态势综述

1. 漏洞总量与趋势

从 2020 年至 2024 年披露的漏洞数据可以看出，通用软件漏洞的年度披露总量呈现出显著的波动和持续增长趋势。2021 年披露的漏洞数量有所下降，为 22,809 个，但随后逐年上升，尤其是 2024 年，漏洞数量大幅增长至 44,957 个，比 2023 年增长超过了 50%。这一趋势可能反映了漏洞挖掘技术的进步、信息安全意识的增强以及更多软件系统被纳入安全审查范围。

数据表明，软件开发和使用的复杂性增加，加之更多企业和机构主动披露漏洞，导致漏洞数量高速增长。这也突显了网络安全形势的日益严峻。对于企业和开发者而言，这一趋势提出了更高的安全管理要求。

建议企业强化软件开发过程中的安全评估，实施“安全左移”策略，将安全测试融入开发生命周期。同时，积极关注漏洞披露平台和行业安全动态，及 时更新系统和补丁。此外，应持续加强人员培训与演练，提升应急响应能力，确保能够快速应对漏洞可能带来的威胁。通过建立完善的安全治理体系，企业可以更有效地适应快速变化的安全环境。

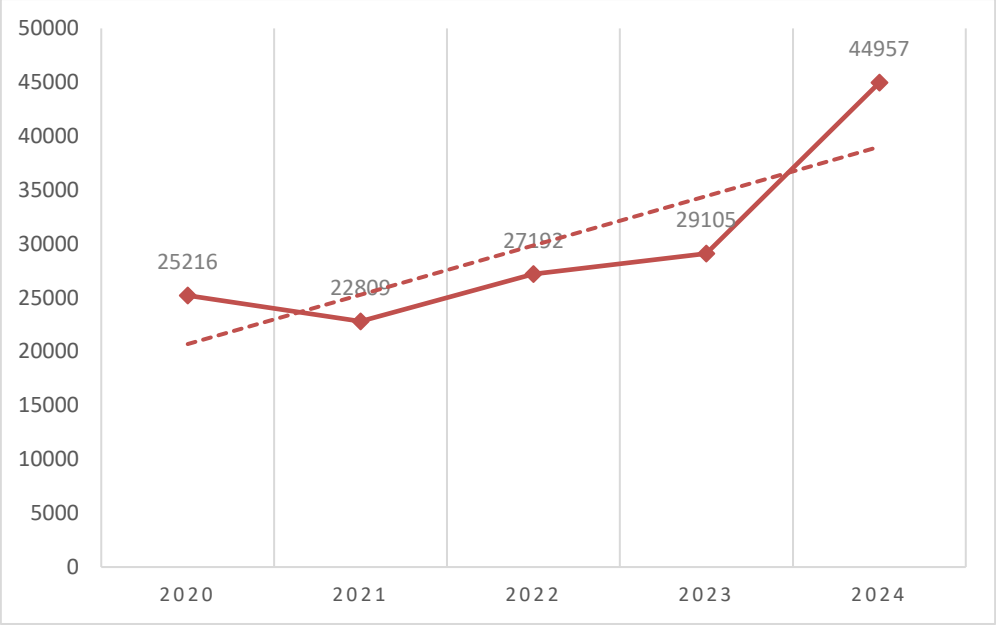

图 1 漏洞总量年度增长趋势图

2. 人工深运营情报数据分析

在 2024 年，360 漏洞情报通过对全球范围内披露的超 4 万条通用软件漏洞进行综合分析，结合使用广度、行业关注度、客户关注度、漏洞攻击复杂度和补丁发布情况等多维度指标，以及 360 漏洞 AI 模型与人工研判，累计输出了 800 余条需要用户高度关注且需要快速修复的漏洞情报。其中，国产软件漏洞 400 余条，国外软件漏洞 400 余条，开源软件漏洞 200 余条。而在这些漏洞中，约有 600 条高度易被利用，300 余条为需尽快修复的高危漏洞。可以看出，高风险漏洞数量仍在逐年递增，对企业防护能力提出了更高的要求。

在 2024 年的攻防演练期间，360 漏洞情报团队累计捕获了 80,702 条漏洞攻击样本，发布漏洞情报预警 180 余条（企业用户可登录 360 漏洞云情报平台查看），其中 98%以上属于高危或严重级别漏洞，针对国内软件产品的漏洞占比尤为突出，高达 160 余条。尤其需要注意的是，攻击者在此次攻防演练中所利用的漏洞类型（见图 2）集中在 SQL 注入、文件上传限制不当、路径遍历、命令注入、反序列化和代码注入等方面。其中，SQL 注入以 37%的占比成为使用率最高的漏洞。紧随其后的是文件上传限制不当和路径遍历，分别占比 15%和 8%。通过针对这些漏洞类型的关键特征加强防护，企业可以有效降低 80%以上的漏洞攻击风险。

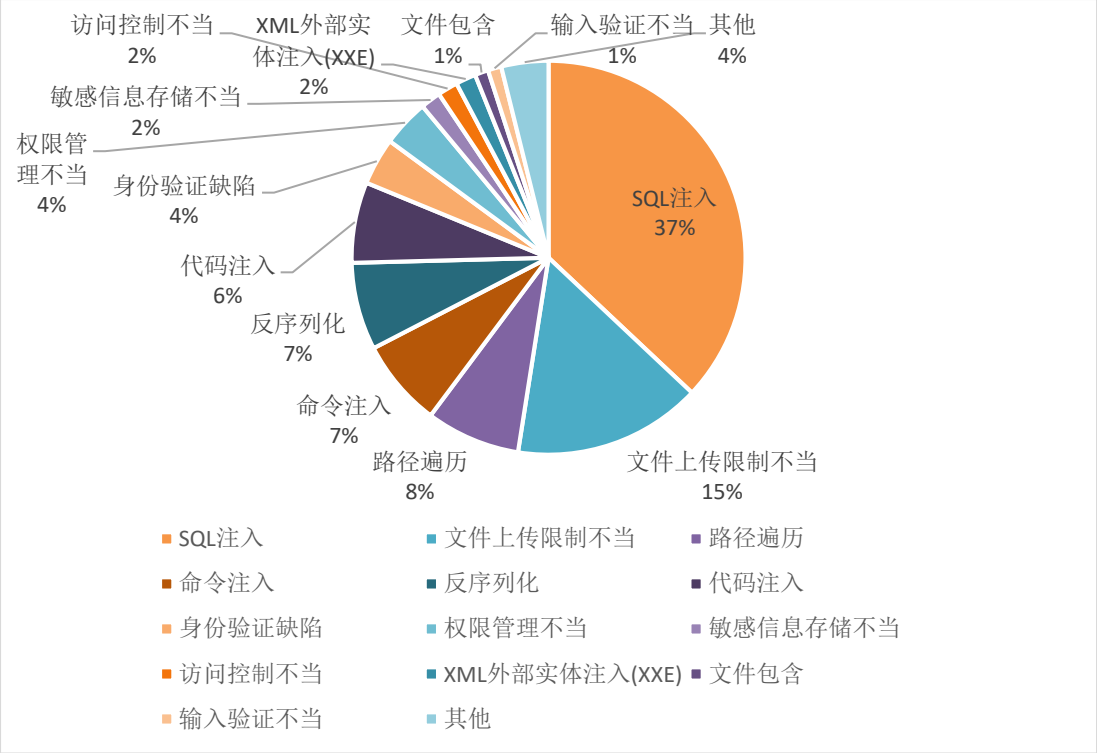

图 2 2024 攻防演练期间漏洞类型利用率占比图

同时，分析显示（见图 3），被攻击者重点关注的产品类型与企业的核心业务系统高度相关。办公自动化系统（OA）成为被攻击最频繁的产品类型，漏洞数量高达 41 个，远超其他系统。其次是企业综合管理系统（21 个漏洞）和企业资源计划系统（ERP）（11 个漏洞）。人力资源管理系统（HRM）和客户关系管理系统（CRM）同样是攻击者青睐的目标，分别存在 10 个和 9 个漏洞。此外，文档管理系统、资产管理系统（EAM）、网关以及大数据处理等产品也存在一定数量的漏洞。可以看出，攻击者往往更倾向于针对企业日常运营中涉及广泛、数据密集的业务系统发起攻击，这些系统一旦被攻破，将对企业的正常运行和数据安全造成严重威胁。

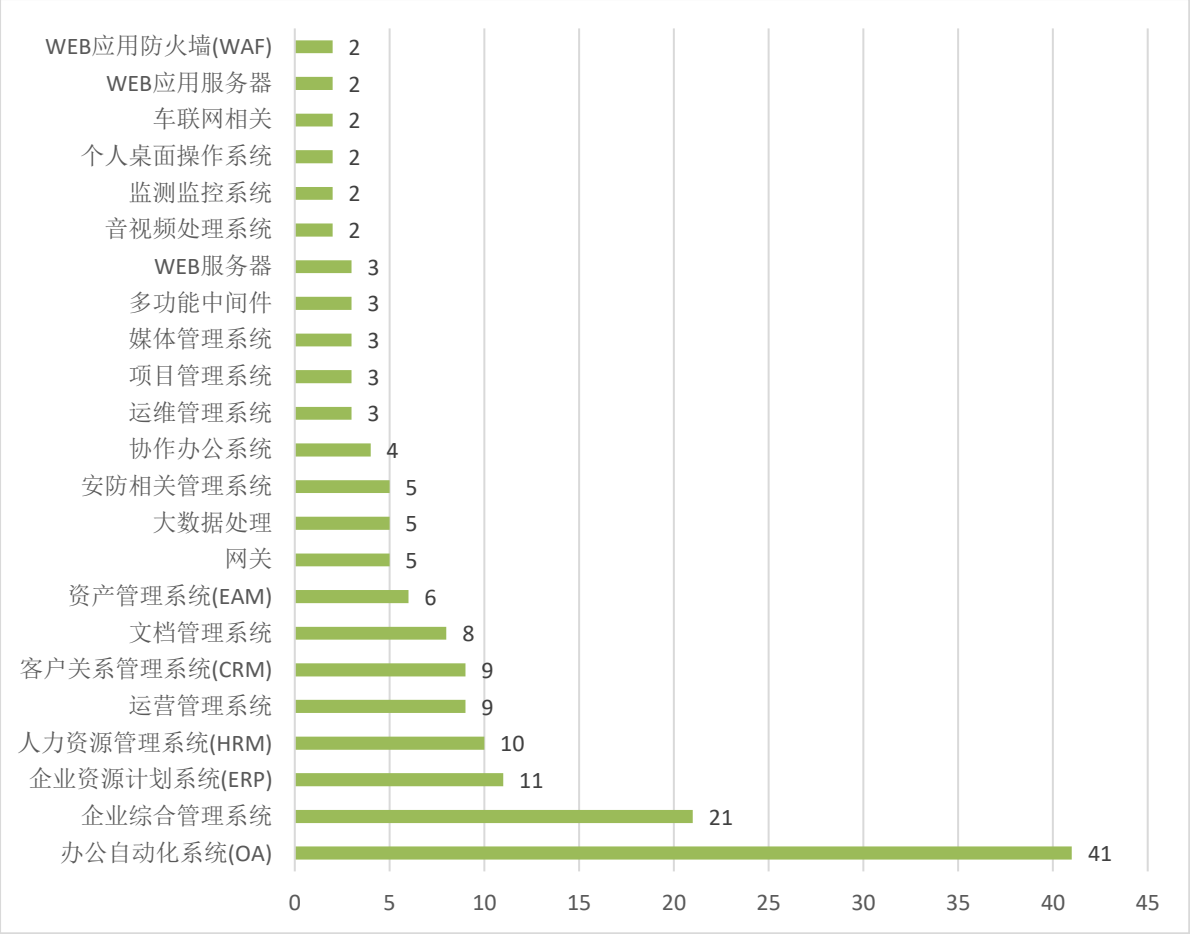

图 3 攻防演练期间被重点攻击的产品分类及对应漏洞数量统计表

360 漏洞情报服务在这些漏洞利用的第一时间，均以最快速的方式提供了临时应急方案，以便用户快速应对攻击威胁，漏洞信息和修复方案均可在情报平台查阅。企业在日常运行中，为了应对这些风险，需重点加强对高风险业务系统的安全防护。特别是针对办公自动化系统（OA）、企业综合管理系统和 ERP 系统等，应定期开展漏洞扫描，及时修复已知漏洞，并对这些核心系统实施网络分区隔离，减少攻击面。同时，针对高频攻击漏洞类型，如 SQL 注入、文件上传限制不当和路径遍历等，应引入更为主动的防御策略，例如部署 Web 应用防火墙（WAF）实时拦截攻击行为，以及对内部开发的软件进行严格的安全审计，确保输入验证的完整性，从源头上降低漏洞被利用的风险。

除了技术层面的安全防护工作，企业还需完善漏洞管理机制，建立快速响应流程，对高危漏洞进行优先级修复，确保补丁及时上线。同时，可通过订阅漏洞情报服务，定期进行渗透测试和安全评估，主动发现潜在的安全隐患。此外，部署完善的数据备份与恢复机制是必不可少的安全保障措施，以应对因恶意攻击导致的关键数据丢失问题。

3. 漏洞披露时间分析

根据 2024 年通用软件漏洞的披露数据显示（图 4），全年的漏洞数量并不均匀，尤其是 10 月份出现了大幅上升，达到了 14,637 个。这一激增可能反映了一个或多个因素，如大量漏洞在经过较长时间的挖掘和处理后集中披露，或者某些重要软件更新导致的漏洞被广泛发现和修复。其余月份的漏洞数量则相对稳定，通常维持在 2,000 至 3,500 之间，这显示出在常规审核和修复节奏下的正常波动。

从数据中可以分析出，漏洞的集中披露可能与行业内的周期性活动、事件或版本更新有关。企业和开发者需要注意这些周期，以便提前做好准备，包括加强漏洞挖掘和修复资源的配置以及提升应急响应能力。建议企业实施持续的安全监控和风险评估，不仅在高风险月份做好防范措施，还需在全年来保持警惕。此外，加强对员工的安全意识培训和演练也是非常必要的，以确保在漏洞披露前后能够灵活应对潜在威胁。通过这些策略，企业可以更加有效地保护其信息系统的安全性。

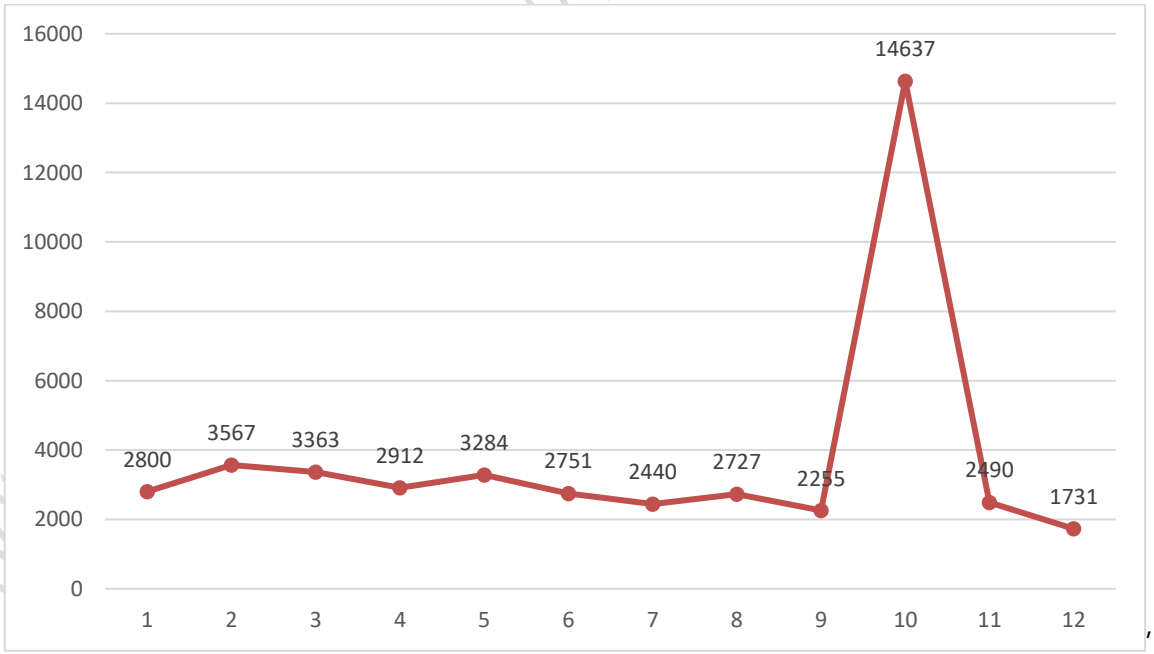

图 4 2024 年每月漏洞数量分布图

4. 漏洞严重程度分析

2024 年通用软件漏洞按照严重性等级的统计数据显示（如表 1、图 5），中危级别的漏洞占据最大比例，共有 18,639 个，占总数的显著份额。这表明在软件系统中，存在大量需要关注但不至于立刻影响系统整体安全的风险。此外，高危（11,786 个）和严重（10,873 个）漏洞的数量也不容忽视，这些漏洞对系统安全构成了直接威胁，需优先处理。

从数据中可以分析出，尽管中危漏洞数量最多，但高危和严重漏洞带来的潜在威胁更为紧迫。企业在安全策略上应优先考虑对高危和严重漏洞的检测和修复，以防止重大安全事件的发生。同时，对于中危漏洞，建议建立完善的监控和评估机制，及时进行风险评估和修复。低危漏洞也不应被忽视，应在资源允许的情况下逐步解决。通过实施分级处理策略和持续监控，企业可以更有效地管理安全风险，确保信息系统的稳定和安全。

漏洞等级	漏洞数量
严重	10873
高危	11786
中危	18639
低危	2669

表 1 2024 年漏洞严重性等级数量表

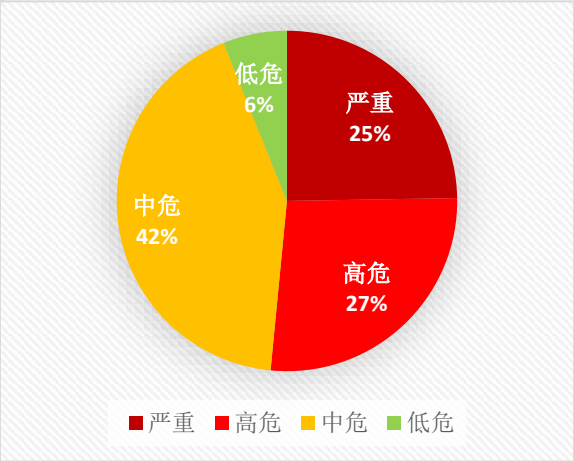

图 5 2024 年漏洞严重性等级占比图

5. 漏洞类型分析

2024 年全年发现的漏洞主要集中在跨站点脚本攻击(XSS)、SQL 注入、权限管理不当、访问控制不当、命令注入、缓冲区溢出、路径遍历、跨站请求伪造(CSRF)、UAF、输入验证不当、越界读取、文件上传限制不当、NULL 指针取消引用、资源分配控制不当、代码注入、中和不当、越界写入、异常处理不当、凭证管理不当、反序列化。表 2 和图 6 展示了 2024 年披露的漏洞数据中排名前 20 的漏洞类型及其占比。

跨站点脚本攻击（XSS）和 SQL 注入是漏洞最多的两种类型，分别有 7,179 和 3,293 个案例。这表明，尽管安全措施不断加强，这两类传统漏洞依然是软件系统中的主要安全挑战。此外，权限管理不当和访问控制不当也占据显著比例，反映出在开发设计阶段，逻辑安全问题需要被重点关注。

企业在开发和维护软件时，需要特别关注这些高风险漏洞类型，首先实施严格的输入验证和输出编码，防止跨站点脚本攻击（XSS）和恶意代码注入。其次，使用预处理语句和存储过程，以防止 SQL 注入，确保数据库查询的安全性。权限管理方面，遵循最小权限原则，定期审核和更新权限设置，防止不当访问。加强访问控制，采用多因素认证和细粒度权限配置，确保用户只能访问其授权范围内的资源。为了预防安全漏洞，定期为开发团队提供安全编码实践培训，提高其安全意识和技能。此外，集成自动化安全测试工具，进行持续的代码审查和渗透测试，以便及时发现和修复潜在的安全隐患，也可以购买第三方漏洞情报服务，及时获取最新的软件漏洞信息，及时修补漏洞。通过这些措施，企业可以显著增强软件系统的安全性和可靠性。

漏洞类型 ID	漏洞类型	漏洞数量
VT-110100	跨站点脚本攻击(XSS)	7179
VT-110300	SQL 注入	3293
VT-120100	权限管理不当	2957
VT-120000	访问控制不当	2101
VT-110500	命令注入	2053
VT-130103	缓冲区溢出	1633
VT-110400	路径遍历	1121
VT-120201	跨站请求伪造(CSRF)	997
VT-130201	UAF	987
VT-130400	文件上传限制不当	969
VT-110200	输入验证不当	934
VT-130102	越界读取	884
VT-130202	NULL 指针取消引用	851
VT-130300	资源分配控制不当	840
VT-110600	代码注入	740
VT-110000	中和不当	435
VT-130101	越界写入	428
VT-180000	异常处理不当	385
VT-120202	凭证管理不当	378
VT-110800	反序列化	370
--	其他	4355

表 2　2024 年漏洞类型及数量表

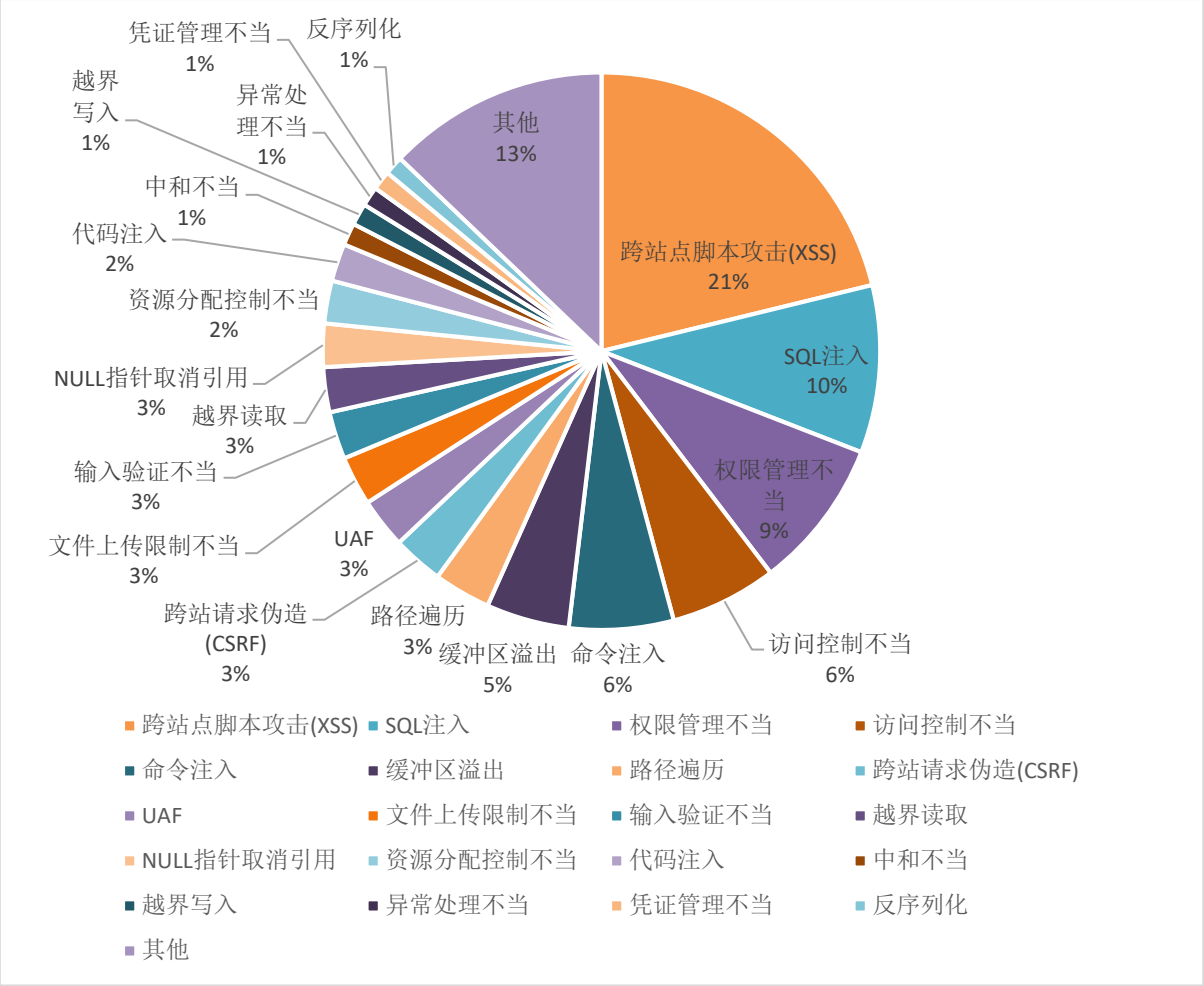

图 6 2024 年漏洞类型占比图

6. 行业漏洞数据分析

360 漏洞情报根据不同的攻防场景和漏洞利用特征，制定了针对攻防场景下的行业分类标准，并对所有漏洞数据进行了行业标注。2024 年的行业漏洞数据统计（见表 3）揭示了各行业面临的不同程度安全威胁。其中，通用行业报告了 40,156 个漏洞，这一庞大数字反映出广泛使用的软件系统在不同行业中普遍存在的安全隐患。由于通用软件并非专用于特定行业，其高风险性对多个领域的运营和数据安全产生了广泛影响。

教育行业出现了 869 个漏洞，显示出数字化教学环境中的安全问题。批发和零售业的 696 个漏洞强调了在线交易平台需要更加稳固的安全保障。金融业与医疗行业分别报告了 585 和 333 个漏洞，指出了保护金融数据和患者信息的紧迫性。

跨行业的软件安全是一个亟待解决的重要问题。建议各行业加强对通用软件的安全管理，实施更严格的漏洞扫描和定期更新策略。特别是在数据敏感的领域，必须引入先进的安全能力，

如威胁情报、漏洞情报，以提升整体防护能力。此外，企业增加信息安全岗位的设置、加强员工的信息安全培训也是降低安全风险、提升应对能力的重要措施。通过这些综合措施，能够有效降低漏洞风险，确保各行业的信息安全和业务连续性。

行业	漏洞数量
PCIC-1 通用行业	40156
PCIC-3 教育	869
PCIC-19 批发和零售业	696
PCIC-2 金融业	585
PCIC-4 医疗卫生和社会工作	333
PCIC-14 住宿和餐饮业	323
PCIC-10 制造业	320
PCIC-12 广播、电视、电影和录音制作业	302
PCIC-7 国家机构	275
PCIC-13 交通运输、仓储和邮政业	255
PCIC-17 租赁和商务服务业	227
PCIC-6 电力、热力、燃气及水生产和供应业	227
PCIC-16 房地产业	177
PCIC-5 电信、广播电视和卫星传输服务	163
PCIC-15 建筑业	146
PCIC-18 农、林、牧、渔业	109
PCIC-21 居民服务、修理和其他服务业	104
PCIC-9 铁路、船舶、航空航天和其他运输设备制造业	95
PCIC-20 水利、环境和公共设施管理业	67
PCIC-8 汽车制造业	47
PCIC-11 采矿业	23

表 3 2024 年行业通用漏洞数量表

7. 受漏洞影响产品分析

图 7 基于 2024 年披露的通用软件漏洞数据，展示了漏洞数量超过 100 的单个产品的分布情况。图中显示 Linux Kernel 以 4531 个漏洞位居榜首，显示出其在安全性方面的巨大挑战。Windows 系列产品也表现出较高的漏洞数量，尤其是 Windows 10 和 Windows 11，分别有 1244 和 1011 个漏洞。此外，Adobe Experience Manager、Google Chrome 和 WordPress 等常用软件也存在较多的安全漏洞。

数据表明，操作系统和广泛使用的应用程序仍是安全漏洞的主要聚集点。高风险软件往往与其复杂性和广泛的用户基础有关，这意味着即便经过多次更新和修复，漏洞仍可能出现。

使用这些软件的企业应部署全面的安全策略，包含定期更新、漏洞扫描和风险评估。此外，推进与安全研究机构的合作，提升漏洞响应速度和修复质量，可以有效减小安全风险，保障用户的数据信息安全。

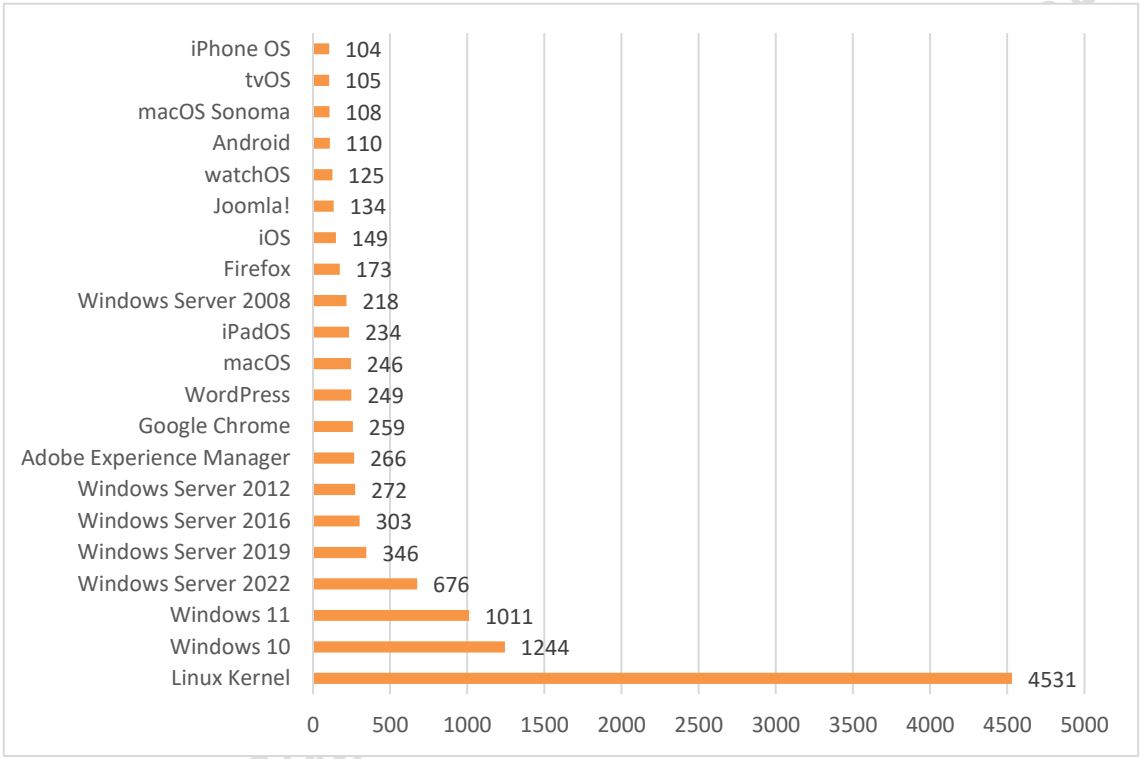

图 7 2024 年漏洞数量超过 100 的产品分布图

三、 重点漏洞列表

以下是 360 漏洞情报根据 2024 年爆发的几万条安全漏洞，通过深度分析漏洞的破坏性、漏洞利于条件、漏洞利用结果等维度，综合评估处出的需要企业重点关注的安全漏洞，共 65 条。

1. Gitlab Gitlab 访问控制不当漏洞

漏洞编号 LDYVUL-2024-00003169 、 CVE-2023-7028
漏洞等级 严重
漏洞类型 访问控制不当
漏洞时间 2024-01-12 15:04:55
在野利用 存在

GitLab 是美国 GitLab 公司的一个开源的端到端软件开发平台,具有内置的版本控制、问题跟踪、代码审查、CI/CD（持续集成和持续交付）等功能。GitLab 存在安全漏洞，该漏洞源于用户帐户密码重置电子邮件可能会发送到未经验证的电子邮件地址。

2. Atlassian Confluence 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00003744 、 CVE-2023-22527
漏洞等级 严重
漏洞类型 代码注入
漏洞时间 2024-01-16 15:15:38
在野利用 存在

360 漏洞云监测到 Atlassian 发布安全公告，其中公开了一个 Confluence 协作平台的代码注入漏洞，允许未经身份验证的攻击者在服务器上实现执行任意代码，获取服务器控制权限。

3. Ivanti Connect Secure 需授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00003241 、 CVE-2024-21887
漏洞等级 严重
漏洞类型 命令注入
漏洞时间 2024-01-17 17:57:31
在野利用 存在

Ivanti Connect Secure 是美国 Ivanti 公司的安全远程网络连接工具。Ivanti Connect Secure 9.x、22.x 系列版本、 Ivanti Policy Secure 9.x、22.x 系列版本存在命令注入漏洞，该漏洞源于 Web 组件中存在命令注入，允许经过身份验证的管理员发送特制请求并在设备上执行任意命令。

4. Jenkins 未授权 路径遍历漏洞 可导致敏感信息泄露

漏洞编号 LDYVUL-2024-00005937 、 CVE-2024-23897
漏洞等级 高危
漏洞类型 路径遍历
漏洞时间 2024-01-25 16:11:10

360 漏洞云监测到 Jenkins 团队发布安全公告,其中公开了一个未授权路径遍历漏洞,该漏洞源于允许未经身份验证的攻击者读取 Jenkins 控制器文件系统,导致敏感信息泄露。

5. Minio Minio 权限管理不当漏洞

漏洞编号 LDYVUL-2024-00007411 、 CVE-2024-24747
漏洞等级 高危
漏洞类型 权限管理不当
漏洞时间 2024-02-01 18:02:57
在野利用 存在

MinIO 是美国 MinIO 公司的一款开源的对象存储服务器。该产品支持构建用于机器学习、分析和应用程序数据工作负载的基础架构。

MinIO 存在安全漏洞。攻击者利用该漏洞可以获得更高的权限。

6. Ivanti Connect Secure 权限管理不当漏洞

漏洞编号 LDYVUL-2024-00003232 、 CVE-2023-46805
漏洞等级 高危
漏洞类型 权限管理不当
漏洞时间 2024-02-01 18:50:49

Ivanti ICS 是美国 Ivanti 公司的一代远程安全访问产品。Ivanti ICS 9.x 版本、22.x 版本、Ivanti Policy Secure 存在授权问题漏洞，该漏洞源于 Web 组件中存在身份验证绕过漏洞。攻击者利用该漏洞可以绕过控制检查来访问受限资源。

7. Oracle Weblogic Server 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00011935 、 CVE-2024-20931
漏洞等级 高危
漏洞类型 代码注入
漏洞时间 2024-02-06 18:09:57

Oracle Fusion Middleware（Oracle 融合中间件）和 Oracle WebLogic Server 都是美国甲骨文（Oracle）公司的产品。Oracle Fusion Middleware 是一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Oracle WebLogic Server 是一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。360 漏洞云监测到 Oracle Fusion Middleware 的 Oracle WebLogic Server 12.2.1.4.0 版本、14.1.1.0.0 版本存在一个代码注入漏洞。攻击者利用该漏洞可以获取服务器控制权限。

8. Microsoft Exchange Server 权限管理不当漏洞可导致权限提升

漏洞编号 LDYVUL-2024-00010775 、 CVE-2024-21410
漏洞等级 严重
漏洞类型 权限管理不当
漏洞时间 2024-02-22 16:10:35
在野利用 存在

Microsoft Exchange Server 是美国微软(Microsoft)公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。

Microsoft Exchange Server 存在安全漏洞。以下产品和版本受到影响：Microsoft Exchange Server 2016 Cumulative Update 23,Microsoft Exchange Server 2019 Cumulative Update 13,Microsoft Exchange Server 2019 Cumulative Update 14。

9. Jetbrains Teamcity 身份验证缺陷漏洞

漏洞编号 LDYVUL-2024-00016777 、 CVE-2024-27198
漏洞等级 严重
漏洞类型 身份验证缺陷
漏洞时间 2024-03-05 15:06:09

JetBrains TeamCity 是捷克 JetBrains 公司的一套分布式构建管理和持续集成工具。该工具提供持续单元测试、代码质量分析和构建问题分析报告等功能。JetBrains TeamCity 2023.11.4 之前版本存在安全漏洞，该漏洞源于存在身份验证绕过漏洞。

10. Apple Macos 越界写入漏洞

漏洞编号 LDYVUL-2024-00018853 、 CVE-2024-23296
漏洞等级 高危

漏洞编号　LDYVUL-2024-00018853 、 CVE-2024-23296
漏洞类型　越界写入
漏洞时间　2024-03-06 17:09:08
在野利用　存在

Apple iOS 和 Apple iPadOS 都是美国苹果（Apple）公司的产品。Apple iOS 是一套为移动设备所开发的操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Apple iOS 17.4 版本和 iPadOS 17.4 版本存在安全漏洞，该漏洞源于具有任意内核读写能力的攻击者可能能够绕过内核内存保护。

11. Adobe ColdFusion 未授权 任意文件读取漏洞

漏洞编号　LDYVUL-2024-00021457 、 CVE-2024-20767
漏洞等级　高危
漏洞类型　输入验证不当
漏洞时间　2024-03-26 17:00:03

Adobe ColdFusion 存在任意文件读取漏洞，漏洞原因在于 Adobe ColdFusion 中存在一处访问控制不当，未经身份认证的远程攻击者可以构造恶意请求读取目标服务器上的任意文件，泄露敏感信息。

12. Palo Alto Networks Pan-Os 未授权 命令注入漏洞

漏洞编号　LDYVUL-2024-00520293 、 CVE-2024-3400
漏洞等级　严重
漏洞类型　命令注入
漏洞时间　2024-04-13 15:10:45

360 漏洞云监测到 Palo Alto Networks PAN-OS 中存在一个命令注入漏洞，未经身份验证的攻击者可利用该漏洞在防火墙上以 root 权限执行任意代码，该漏洞影响启用了 GlobalProtect 网关的 PAN-OS 10.2、PAN-OS 11.0 和 PAN-OS 11.1 防火墙，导致未经身份验证的攻击者可利用该漏洞在防火墙上以 root 权限执行任意代码，Cloud NGFW、Panorama 设备和 Prisma Access 不受此漏洞的影响。漏洞编号：CVE-2024-3400，漏洞威胁等级：严重。

13. Oracle Weblogic Server 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00520420 、 CVE-2024-21006
漏洞等级 高危
漏洞类型 代码注入
漏洞时间 2024-04-17 16:06:33

360 漏洞云监测到 Oracle 发布了四月安全公告，其中存在一个 Oracle WebLogic Server 远程代码执行漏洞，未经身份验证的攻击者可以利用该漏洞在远程服务器上执行任意代码，漏洞编号：CVE-2024-21006，漏洞威胁等级：高危。该漏洞是由于当 weblogic 开启 T3/IIOP 协议时，攻击者可以向协议的监听端口发送恶意数据，进而在服务上执行任意代码，导致对关键数据的未授权访问或对所有 Oracle WebLogic Server 可访问数据的完全访问。

14. 凯京信达 Kkfileview 未授权 文件上传限制不当漏洞

漏洞编号 LDYVUL-2024-00520428
漏洞等级 严重
漏洞类型 文件上传限制不当
漏洞时间 2024-04-17 18:04:09

360 漏洞云监测到 kkFileView 存在一个任意文件上传漏洞，攻击者可利用该漏洞上传恶意文件，获取操作系统权限。

15. CrushFTP 团队 Crushftp 未授权 模板注入漏洞

漏洞编号 LDYVUL-2024-00526825 、 CVE-2024-4040
漏洞等级 严重
漏洞类型 文件上传限制不当
漏洞时间 2024-04-25 17:33:56

360 漏洞云监测到 CrushFTP 在 10.7.1 之前的 v10 版本 、11.1.0 版本之前的 v11 版本和 v7，v8，v9 全版本存在一个未授权的服务端模板注入漏洞，未授权的攻击者可以

通过该漏洞读取服务器的敏感文件，甚至在服务器上执行任意代码。漏洞编号：CVE-2024-4040，漏洞威胁等级：严重。该漏洞是由于 CrushFTP 未能正确处理用户输入，将用户输入直接带入了模板引擎中执行，导致用户可以注入恶意代码来加载任意文件，并可以通过读取 session 文件获取管理员用户凭证登录。

16. Google Chrome Visual 释放后利用漏洞可导致程序崩溃

漏洞编号 LDYVUL-2024-00538020 、 CVE-2024-4671
漏洞等级 严重
漏洞类型 UAF
漏洞时间 2024-05-10 16:09:53
在野利用 存在

Google Chrome Visual 中存在一处释放后利用漏洞，此类漏洞通常会在成功破坏堆内存后导致浏览器崩溃或执行任意代码。

17. Google Chrome 越界写入

漏洞编号 LDYVUL-2024-00260076 、 CVE-2024-4761
漏洞等级 高危
漏洞类型 越界写入
漏洞时间 2024-05-16 16:18:43

Chrome V8 中的越界写入漏洞，此类漏洞通常会在成功破坏堆内存后，导致浏览器崩溃或执行任意代码

18. Sonatype Nexus Repository 未授权 路径遍历漏洞

漏洞编号 LDYVUL-2024-00261614 、 CVE-2024-4956
漏洞等级 高危
漏洞类型 路径遍历
漏洞时间 2024-05-22 18:23:36

Sonatype Nexus Repository 3.68.1 之前版本存在安全漏洞，该漏洞源于存在路径遍

历，允许未经身份验证的攻击者读取系统文件。

19. Google Chrome 类型混淆漏洞

漏洞编号 LDYVUL-2024-00266072 、 CVE-2024-5274
漏洞等级 高危
漏洞类型 类型混淆
漏洞时间 2024-05-24 16:48:08
在野利用 存在

Chrome V8 中的存在类型混淆漏洞，此类漏洞通常会在成功破坏堆内存后，导致浏览器崩溃或执行任意代码。目前，此漏洞已检测到在野利用。

20. Fortinet Fortiproxy 越界写入漏洞可导致远程代码执行

漏洞编号 LDYVUL-2024-00009715 、 CVE-2024-21762
漏洞等级 严重
漏洞类型 越界写入
漏洞时间 2024-05-31 10:30:51

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 存在缓冲区错误漏洞，该漏洞源于存在越界写入，允许攻击者通过特制请求执行未经授权的代码或命令。

21. Check Point Security Gateways 未授权 任意文件读取漏洞

漏洞编号 LDYVUL-2024-00267040 、 CVE-2024-24919
漏洞等级 高危
漏洞类型 访问控制不当
漏洞时间 2024-06-03 15:43:58

Check Point Security Gateways 是以色列 Check Point 公司的一个人工智能驱动的 NGFW 安全网关。Check Point Security Gateways 存在一个任意文件读取漏洞。攻击者利用该漏洞可以获取敏感信息。

22. Apache OFBiz 未授权 路径遍历漏洞 可导致远程代码执行

漏洞编号 LDYVUL-2024-00537165 、 CVE-2024-32113
漏洞等级 严重
漏洞类型 路径遍历
漏洞时间 2024-06-04 16:26:15

Apache OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache OFBiz 18.12.13 之前版本存在路径遍历漏洞，该漏洞的存在是由于 Apache Ofbiz 受限目录路径名不正确限制,产生路径遍历漏洞，导致攻击者可以通过构造恶意路径请求后端接口执行恶意代码。

23. Linux Linux Kernel UAF 漏洞 可致本地权限提升

漏洞编号 LDYVUL-2024-00007218 、 CVE-2024-1086
漏洞等级 高危
漏洞类型 UAF
漏洞时间 2024-06-06 09:27:42

Linux kernel 存在安全漏洞，该漏洞源于 netfilter: nf_tables 组件中存在释放后重用，nf_hook_slow() 函数可能会导致双重释放，攻击者利用该漏洞导致本地权限提升。

24. Progress Software Telerik Report Server 身份验证缺陷漏洞

漏洞编号 LDYVUL-2024-00267272 、 CVE-2024-4358
漏洞等级 严重
漏洞类型 身份验证缺陷

漏洞编号 LDYVUL-2024-00267272 、 CVE-2024-4358
漏洞时间 2024-06-06 15:22:35

Progress Software Telerik Report Server 是 Progress Software 公司的一种企业级报表管理和分发解决方案。Progress Software Telerik Report Server 10.0.24.305 及之前版本存在安全漏洞，该漏洞源于未经身份验证的攻击者可以通过身份验证绕过漏洞访问受限功能。

25. PHP CGI 代码注入漏洞

漏洞编号 LDYVUL-2024-00270053 、 CVE-2024-4577
漏洞等级 严重
漏洞类型 命令注入
漏洞时间 2024-06-07 14:55:54
在野利用 存在

360 漏洞云监测到 PHP 存在一个代码注入漏洞，当 PHP 的 PHP-CGI 模式运行在 Window 平台且使用了特定语系时，攻击者可构造恶意请求绕过 CVE-2012-1823 补丁，通过注入恶意的 CGI 模式命令参数，在服务上执行任意 PHP 代码。

26. SolarWinds ServU 路径遍历漏洞

漏洞编号 LDYVUL-2024-00269513 、 CVE-2024-28995
漏洞等级 高危
漏洞类型 路径遍历
漏洞时间 2024-06-14 14:51:17

SolarWinds Serv-U File Server 是美国 SolarWinds 公司的一款文件传输服务器。SolarWinds Serv-U 存在路径遍历漏洞，未经身份认证的远程攻击者通过构造恶意请求可以访问读取主机上的敏感文件，对服务器机密性造成较高影响。

27. Adobe Commerce 未授权 外部实体注入漏洞

漏洞编号 LDYVUL-2024-00380448 、 CVE-2024-34102
漏洞等级 严重
漏洞类型 XML 外部实体注入(XXE)
漏洞时间 2024-06-17 14:59:42
在野利用 存在

Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。Adobe Commerce 存在一个 XML 外部实体引用（ XXE ）漏洞，同时该漏洞也影响开源版本 Magento Open Source，未经授权的攻击者成功利用该漏洞可能导致任意代码执行。

28. Zyxel NAS 未授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00268743 、 CVE-2024-29973
漏洞等级 严重
漏洞类型 命令注入
漏洞时间 2024-06-20 10:26:11

Zyxel NAS326 V5.21(AAZF.17)C0 之前版本、NAS542 V5.21(ABAG.14)C0 之前版本存在操作系统命令注入漏洞，该漏洞源于 setCookie 参数中存在命令注入漏洞，从而导致攻击者可通过 HTTP POST 请求来执行某些操作系统 (OS) 命令。

29. Rejetto HTTP File Server 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00267966 、 CVE-2024-23692
漏洞等级 严重
漏洞类型 代码注入
漏洞时间 2024-06-21 16:27:43
在野利用 存在

Rejetto HTTP 文件服务器在旧版本中（<=2.4.0 RC7）存在一个代码注入漏洞。此漏洞允许远程未经身份验证的攻击者通过发送特制的 HTTP 请求在受影响的系统上执行任

意命令。自 CVE 分配日期起，Rejetto HFS 2.x 版本已经不再受支持。

30. GeoServer 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00385396 、 CVE-2024-36401
漏洞等级 严重
漏洞类型 代码注入
漏洞时间 2024-07-03 10:15:18
在野利用 存在

GeoServer 是一个开源服务器，允许用户共享和编辑地理空间数据。GeoServer 在版本 2.23.6、2.24.4 和 2.25.2 之前，允许未经身份验证的用户通过多个 OGC 请求参数针对默认 GeoServer 安装的特别构造的输入利用代码注入漏洞，该漏洞是由于应用不安全地将属性名称作为 XPath 表达式进行评估，攻击者可以在默认安装的服务器中执行 XPath 表达式，进而利用执行 Apache Commons Jxpath 提供的功能执行任意代码。

31. ServiceNow 未授权 模板注入漏洞

漏洞编号 LDYVUL-2024-00388809 、 CVE-2024-4879
漏洞等级 严重
漏洞类型 输入验证不当
漏洞时间 2024-07-11 18:58:19

ServiceNow 的 Jelly 模板和 Glide 表达式由于输入验证不严格，存在一个模板注入漏洞。这些漏洞可以被未经身份验证的攻击者通过构造恶意请求利用，在 ServiceNow 中远程执行代码。

32. ServiceNow 未授权 输入验证不当漏洞

漏洞编号 LDYVUL-2024-00388817 、 CVE-2024-5217
漏洞等级 严重
漏洞类型 中和不当
漏洞时间 2024-07-12 15:16:14

ServiceNow 的 Washington DC、Vancouver 和 Utah Now Platform 平台版本中存在一个输入验证错误漏洞。此漏洞可能使未经身份验证的用户在 Now Platform 环境中远程执行代码。

33. 1Panel 未授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00391565 、 CVE-2024-39911
漏洞等级 严重
漏洞类型 SQL 注入
漏洞时间 2024-07-22 15:21:42

1Panel 是一个基于 Web 的 Linux 服务器管理控制面板。1Panel 1.10.12-tls 之前的版本存在 SQL 注入漏洞，该漏洞的成因是 1Panel 对 User-Agent 头处理时缺乏安全过滤导致了 sql 注入漏洞。

34. Apache OFBiz 未授权 代码注入漏洞

漏洞编号 LDYVUL-2024-00535316 、 CVE-2024-38856
漏洞等级 严重
漏洞类型 代码注入
漏洞时间 2024-08-05 16:57:05

Apache OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。Apache OFBiz 18.12.14 及之前版本存在安全漏洞，该漏洞源于存在授权错误漏洞，从而导致未经身份验证的端点可执行屏幕渲染代码。

35. Microsoft Edge 类型混淆漏洞

漏洞编号 LDYVUL-2024-00536992 、 CVE-2024-38178
漏洞等级 高危

漏洞编号　LDYVUL-2024-00536992 、 CVE-2024-38178
漏洞类型　类型混淆
漏洞时间　2024-08-14 11:23:00

Microsoft Edge 浏览器的 Internet Explorer 模式中存在一个 Jscript9 脚本引擎内存损坏漏洞，当用户使用 Edge 浏览器的 IE 模式并点击特制链接时，攻击者可以在目标系统上执行任意代码，该漏洞存在在野利用。

36. 宝兰德软件 BES 管理控制台 ejb 未授权 反序列化漏洞 可致远程代码执行

漏洞编号　LDYVUL-2024-00541423
漏洞等级　严重
漏洞类型　反序列化
漏洞时间　2024-08-15 18:31:14

360 漏洞云监测北京宝兰德软件股份有限公司 BES 管理控制台存在一个未授权反序列化漏洞，未经身份验证的攻击者可以通过该漏洞在服务器上执行任意代码，获取服务器控制权限。

37. Google Chrome 类型混淆漏洞

漏洞编号　LDYVUL-2024-00544155 、 CVE-2024-7971
漏洞等级　高危
漏洞类型　类型混淆
漏洞时间　2024-08-22 18:10:59
在野利用　存在

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。V8 是其中的一套开源 JavaScript 引擎。Google Chrome 128.0.6613.84 版本及之前版本存在安全漏洞，该漏洞源于包含一个类型混淆问题。

38. Google Chrome UAF 漏洞

漏洞编号　LDYVUL-2024-00544141 、 CVE-2024-7965
漏洞等级　高危
漏洞类型　UAF
漏洞时间　2024-08-28 16:40:38
在野利用　存在

Chrome 存在释放后重用漏洞（UAF），该漏洞存在于 Chrome 的 V8 JavaScript 引擎中，攻击者可以通过精心构造的 HTML 页面，利用该漏洞远程攻击目标系统，导致浏览器崩溃或执行任意代码。

39. Microsoft Windows 网络标记 设计缺陷漏洞

漏洞编号　LDYVUL-2024-00544625 、 CVE-2024-38217
漏洞等级　中危
漏洞类型　设计缺陷
漏洞时间　2024-09-11 11:13:13
在野利用　存在

360 漏洞云监测到微软发布 9 月安全公告，修复了多个安全漏洞，其中包含一个 Microsoft Windows 网络标记 设计缺陷漏洞。该漏洞是由于安全措施实施不足而存在的。攻击者通过诱骗受害者下载特制文件，逃避 Web 标记 (MOTW) 防御并绕过安全功能，该漏洞存在在野利用。

40. Microsoft Windows Installer 权限管理不当漏洞 可致权限提升

漏洞编号　LDYVUL-2024-00544910 、 CVE-2024-38014
漏洞等级　高危
漏洞类型　权限管理不当
漏洞时间　2024-09-11 12:41:24

漏洞编号 LDYVUL-2024-00544910 、 CVE-2024-38014
在野利用 存在

360 漏洞云监测到微软发布 9 月安全公告，修复了多个安全漏洞，其中包含一个 Microsoft Windows Installer 权限管理不当漏洞，该漏洞是由于 Windows Installer 中的权限管理不当而导致的，攻击者可以利用此漏洞提权到 SYSTEM 权限执行任意代码，该漏洞存在在野利用。

41. Zimbra Collaboration 未授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00546099 、 CVE-2024-45519
漏洞等级 严重
漏洞类型 安全缺陷
漏洞时间 2024-09-13 12:49:16

360 漏洞云监测到 Zimbra Collaboration 发布更新版本，新版本中修复了多个安全漏洞，其中包含 postjournal 服务中的一个命令注入漏洞，在远程 Zimbra 服务器开启了 postjournal 服务时，未经身份验证的攻击者可以利用此漏洞执行系统任意命令，获取服务器控制权限。

42. Ivanti Cloud Services Appliance 需授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00545016 、 CVE-2024-8190
漏洞等级 高危
漏洞类型 命令注入
漏洞时间 2024-09-13 18:29:43
在野利用 存在

360 漏洞云监测到 Ivanti 发布安全公告，修复了 Ivanti Cloud 中的一个命令注入漏洞，该漏洞允许经过身份验证的远程攻击者获取远程代码执行。攻击者必须具有管理员级别的权限才能利用此漏洞。

43. Spring Cloud Data Flow 反序列化漏洞 可导致代码执行

漏洞编号 LDYVUL-2024-00531505 、 CVE-2024-37084
漏洞等级 严重
漏洞类型 反序列化
漏洞时间 2024-09-14 16:05:48

VMware Spring Cloud Data Flow 是美国威睿（VMware）公司的一款用于微服务中流式处理和批处理数据的代码库。VMware Spring Cloud Data Flow 2.11.0 版本至 2.11.3 版本存在一个反序列化漏洞，该漏洞源于有权访问服务器 API 的恶意用户可以使用特制请求将包含恶意数据的 YAML 文件写入文件系统上的指定位置，然后触发该文件进行反序列化操作，导致在服务器上执行任意代码。

44. Windows MSHTML Platform 编码不规范漏洞

漏洞编号 LDYVUL-2024-00544757 、 CVE-2024-43461
漏洞等级 高危
漏洞类型 编码不规范
漏洞时间 2024-09-18 14:58:00

360 漏洞云监测到微软发布 9 月安全公告，修复了多个安全漏洞，其中包含一个 Microsoft Windows MSHTML Platform 编码不规范漏洞，该漏洞是由于对用户提供的数据处理不正确而产生的。远程攻击者可以诱骗受害者访问特制的网站，执行欺骗攻击并可能危及受影响的系统。

45. Ivanti Cloud Service Appliance 未授权 路径遍历漏洞

漏洞编号 LDYVUL-2024-00548522 、 CVE-2024-8963
漏洞等级 严重
漏洞类型 路径遍历
漏洞时间 2024-09-23 16:14:34

Ivanti Cloud Services Appliance(Ivanti CSA)是美国 Ivanti 公司的一种 Internet

应用程序。可通过 Internet 提供安全的通信和功能。360 漏洞云监测到 Ivanti Cloud Services Appliance 4.6 Patch 519 之前版本存在一个路径遍历漏洞，允许远程未经身份验证的攻击者访问受限功能，如果结合之前发布的CVE-2024-8190 漏洞可以达到攻击者未授权获取服务器控制权限的效果。

46. 飞致云 DataEase 未授权 访问控制不当漏洞

漏洞编号 LDYVUL-2024-00029297 、 CVE-2024-30269
漏洞等级 中危
漏洞类型 访问控制不当
漏洞时间 2024-09-30 15:27:04

DataEase 是一个开源的数据可视化分析工具。用于帮助用户快速分析数据并洞察业务趋势，从而实现业务的改进与优化。360 漏洞云监测到 DataEase 在 2.5.1 版本之前，DataEase 未能对请求路径进行正确解析，导致攻击者可以通过构造恶意请求获取服务器数据库配置信息。

47. Ivanti CSA 需授权 SQL 注入漏洞

漏洞编号 LDYVUL-2024-00777546 、 CVE-2024-9379
漏洞等级 中危
漏洞类型 SQL 注入
漏洞时间 2024-10-09 15:36:55
在野利用 存在

360 漏洞云监测到 Ivanti 发布安全公告，修复了 3 个安全漏洞，其中包括一个存在于 CSA 5.0.2 之前版本的的 Web 控制台的 SQL 注入漏洞，具有管理员权限的远程验证攻击者可利用此漏洞运行任意 SQL 语句，该漏洞存在在野利用。

48. Ivanti Ivanti CSA 需授权 路径遍历漏洞

漏洞编号 LDYVUL-2024-00777553 、 CVE-2024-9381
漏洞等级 高危

漏洞编号 LDYVUL-2024-00777553 、 CVE-2024-9381
漏洞类型 路径遍历
漏洞时间 2024-10-09 15:51:47
在野利用 存在

360 漏洞云监测到 Ivanti 发布安全公告，修复了 3 个安全漏洞，其中包括一个路径遍历漏洞，具有管理权限的远程经过身份验证的攻击者绕过限制，访问系统任意文件。该漏洞存在在野利用。

49. Fortinet FortiManager 身份验证缺陷漏洞 可致远程代码执行

漏洞编号 LDYVUL-2024-00784142 、 CVE-2024-47575
漏洞等级 严重
漏洞类型 身份验证缺陷
漏洞时间 2024-10-24 14:35:10
在野利用 存在

360 漏洞云监测到 Fortinet 发布安全公告，修复了 FortiManager 平台中存在的一个身份认证缺陷漏洞，漏洞编号：CVE-2024-47575，漏洞危害等级：严重，Fortinet 确认该漏洞已被利用。该漏洞源于 fgfmsd 守护进程中的认证缺失缺陷，可能允许远程未认证攻击者通过特制请求执行任意命令或代码。鉴于漏洞影响较大，建议受影响用户及时采取防护措施。

50. Google Chrome Dawn 越界写入漏洞 可致远程代码执行

漏洞编号 LDYVUL-2024-00816331 、 CVE-2024-10487
漏洞等级 严重
漏洞类型 越界写入
漏洞时间 2024-10-30 15:57:13

360 漏洞云监测到 Gooogle Chrome 发布紧急更新，修复了两个安全漏洞，其中包括一个危害等级为严重的越界写入漏洞，该漏洞存在于 Chrome Dawn 图形库组件中，攻击者

通过制作恶意的 HTLM 网页问价你，并诱导受害者访问以利用该漏洞，成功利用可能导致程序崩溃、敏感信息泄露或任意代码执行。

51. Vmware Spring Security 访问控制不当漏洞 可致功能失控

漏洞编号 LDYVUL-2024-00815145 、 CVE-2024-38821
漏洞等级 严重
漏洞类型 访问控制不当
漏洞时间 2024-10-31 15:47:48

360 漏洞云监测到 VMware 发布安全公告，其中公开了一个 Spring Security 中的访问控制不当漏洞，在某些情况下，Spring WebFlux 应用程序在静态资源上使用 Spring Security 授权规则时可以绕过对静态资源具有 Spring Security 授权规则的访问控制。

52. Ivanti Endpoint Manager SQL 注入漏洞 可致远程代码执行

漏洞编号 LDYVUL-2024-00821723 、 CVE-2024-50330
漏洞等级 严重
漏洞类型 SQL 注入
漏洞时间 2024-11-14 17:15:14

360 漏洞云监测到 Lvanti 发布安全公告，修复了 Ivanti Endpoint Manager 存在 GetComputerID SQL 注入远程代码执行漏洞，漏洞编号：CVE-2024-50330，漏洞危害等级：严重。漏洞原因是在构建 SQL 查询前对用户提供的字符串缺乏正确验证，允许远程攻击者在受影响的安装上执行任意代码，且无需身份验证。Ivanti 已发布更新来纠正此漏洞，建议受影响用户请及时升级到安全版本。

53. 宝兰德 BES 管理控制台 未授权 反序列化漏洞 可致远程代码执行

漏洞编号 LDYVUL-2024-00822901
漏洞等级 严重
漏洞类型 反序列化
漏洞时间 2024-11-18 10:55:16

360 漏洞云监测到宝兰德软件发布安全公告，其中公开披露了一个反序列化漏洞，由于宝兰德 BES 应用服务器产品 Spark 服务存在一个反序列化漏洞，未授权的攻击者可利用该漏洞绕过反序列化黑名单限制，在服务器上执行任意代码，获取服务器权限。

54. Apache OFBiz 服务器端请求伪造(SSRF)漏洞 可致远程代码执行

漏洞编号 LDYVUL-2024-00822929 、 CVE-2024-47208
漏洞等级 中危
漏洞类型 服务器端请求伪造(SSRF)
漏洞时间 2024-11-18 16:08:14

360 漏洞云监测到 Apache OFBiz 官方发布安全公告，修复漏洞中包括一个服务器端请求伪造漏洞，该漏洞表现为 URL 允许远程使用 Groovy 表达式，可能导致远程代码执行（RCE）。受影响的版本为 Apache OFBiz 在 18.12.17 之前的版本。建议用户升级到 18.12.17 版本以修复该问题。

55. Palo Alto Networks PAN-OS Web 管理界面 权限管理不当漏洞 可致权限失控

漏洞编号 LDYVUL-2024-00823214 、 CVE-2024-0012
漏洞等级 高危

漏洞编号　LDYVUL-2024-00823214 、 CVE-2024-0012
漏洞类型　权限管理不当
漏洞时间　2024-11-19 10:54:18
在野利用　存在

360 漏洞云监测到 Palo Alto Networks 发布安全公告，披露了了 PAN--OS 软件 Web 管理界面中存在认证绕过漏洞，未经身份验证的攻击者如果能够访问管理 Web 界面，就可能获得 PAN-OS 管理员权限，从而执行管理操作、篡改配置，结合利用其他需认证的漏洞可实现系统的完全控制。若按照推荐的最佳实践部署指南，将管理 Web 界面的访问限制为仅受信任的内部 IP 地址，可大大降低此风险。官方已提供此漏洞的修复版本，建议受影响用户及时升级到安全版本。

56. 7-zip 整数溢出漏洞 可致远程代码执行

漏洞编号　LDYVUL-2024-00829381 、 CVE-2024-11477
漏洞等级　高危
漏洞类型　整数溢出
漏洞时间　2024-11-25 10:34:21

360 漏洞云监测到 7-Zip 发布更新版本，新版本中修复了一处解压缩过程中整数下溢导致的远程代码执行漏洞，此漏洞允许远程攻击者在受影响的 7-Zip 安装程序中执行任意代码。具体的缺陷存在于 Zstandard 解压缩的实现中。问题源于对用户提供的数据缺乏适当的验证，这可能导致在写入内存之前发生整数下溢。要利用此漏洞，需要与这个库进行交互。由于 7-Zip 作为开源组件，可集成在其他项目中使用，建议用户排查是否有使用受影响版本的 7-Zip，及时采取防护措施。

57. Zabbix 需授权 SQL 注入漏洞

漏洞编号　LDYVUL-2024-00831380 、 CVE-2024-42327
漏洞等级　严重
漏洞类型　SQL 注入
漏洞时间　2024-11-28 18:05:17

360 漏洞云监测到 Zabbix 官方修复了 Zabbix 中一处需授权 SQL 注入漏洞，Zabbix 前

端的 CUser 类中的 addRelatedObjects 函数未对输入数据进行充分验证和转义，具有访问权限的攻击者可以利用该漏洞执行任意 sql 语句，执行任意代码，导致服务器失陷。

58. H3C SecCenter SMP 未授权 输入验证不当漏洞 可导致远程代码执行

漏洞编号 LDYVUL-2024-00831821
漏洞等级 严重
漏洞类型 输入验证不当
漏洞时间 2024-11-29 14:29:58

360 漏洞云监测到 H3C 发布安全公告，其中披露了一个输入验证不当漏洞，未经授权的攻击者可以通过该漏洞上传文件获取服务器控制权限。

59. SonicWall SMA100 SSLVPN web 管理页面 缓冲区溢出漏洞

漏洞编号 LDYVUL-2024-00833851 、 CVE-2024-45318
漏洞等级 高危
漏洞类型 缓冲区溢出
漏洞时间 2024-12-06 17:14:44

360 漏洞云监测到 SonicWall 发布安全公告，修复多个安全漏洞，其中包括一个位于 SonicWall SMA100 SSLVPN web 管理页面的堆缓冲区溢出漏洞。这个漏洞使得远程攻击者能够引发基于栈的缓冲区溢出，并且有可能导致代码执行。官方已针对此漏洞发布更新版本，建议受影响用户及时升级到安全版本。

60. OpenWrt Attended SysUpgrade/Asu 命令注入漏洞

漏洞编号 LDYVUL-2024-00834609 、 CVE-2024-54143
漏洞等级 高危

漏洞编号 LDYVUL-2024-00834609 、 CVE-2024-54143
漏洞类型 命令注入
漏洞时间 2024-12-10 19:24:56

360 漏洞云监测到 OpenWrt Attended SysUpgrade 中的一处命令注入漏洞细节已经公开，由于 OpenWrt Attended SysUpgrade 在镜像构建过程中，用户提供的软件包名称未经适当处理就被合并到 make 命令中，这可能导致恶意用户将任意命令注入构建过程，从而生成使用合法构建密钥签名的恶意固件镜像，建议使用 OpenWrt Attended SysUpgrade 生成固件的用户注意防范风险。

61. GitLab CE/EE 需授权 输入验证不当漏洞 可导致敏感信息泄露

漏洞编号 LDYVUL-2024-00837571 、 CVE-2024-11274
漏洞等级 高危
漏洞类型 输入验证不当
漏洞时间 2024-12-12 10:23:03

360 漏洞云监测到 Gitlab 发布安全公告，修复了多个安全漏洞，其中包含一个 GitLab Enterprise Edition (EE)/Community Edition(CE)中的输入验证不当漏洞，该漏洞源于当在 kubernetes 代理响应中注入网络错误日志 (NEL) 标头时可能会导致会话数据泄露。

62. Apache Struts2 文件上传限制不当漏洞 可导致远程代码执行

漏洞编号 LDYVUL-2024-00837193 、 CVE-2024-53677
漏洞等级 严重
漏洞类型 文件上传限制不当
漏洞时间 2024-12-12 10:34:39

360 漏洞云监测到 Apache Struts 2 发布安全公告，披露了一个文件上传限制不当漏

洞，该漏洞是由于 Apache Struts2 中的文件上传中存在逻辑缺陷，未经授权的攻击者可以操纵文件上传参数来利用路径遍历，上传可用于执行远程代码的恶意文件，该漏洞是由于框架通过在旧版本的文件上传拦截器来获取上传文件的相关参数，并自动将相关参数注入到用户实现的 Action 中，由于该拦截器因为存在逻辑缺陷，导致获取的相关参数可能是攻击者构造的恶意内容，导致用户获取到恶意参数内容，该拦截器已经被新的文件拦截器所替代，鉴于漏洞影响较大，建议受影响用户及时采取防护措施。

63. Apache Tomcat 条件竞争漏洞 可导致远程代码执行

漏洞编号 LDYVUL-2024-00840174 、 CVE-2024-50379
漏洞等级 严重
漏洞类型 条件竞争
漏洞时间 2024-12-18 11:21:50

360 漏洞云监测到 Apache Tomcat 发布安全公告，其中披露了一个条件竞争漏洞，在特定非默认情况下可能导致远程代码执行。当默认 servlet 可写且文件系统(Windows 系统)不区分大小写时，在负载下对同一文件的并发读取和上传可能绕过 Tomcat 的大小写敏感性检查，使上传的文件被视为 JSP 从而导致远程代码执行。官方已针对此漏洞发布更新版本，建议受影响用户及时升级到安全版本。

64. Webmin Webmin CGI 需授权 命令注入漏洞

漏洞编号 LDYVUL-2024-00841990 、 CVE-2024-12828
漏洞等级 严重
漏洞类型 命令注入
漏洞时间 2024-12-24 16:47:29

360 漏洞云监测到 Webmin 中的严重安全漏洞已经公开，该漏洞源于 CGI 请求处理中的命令注入缺陷，软件未正确清理用户输入。此漏洞需身份验证，低权限用户也可利用，即使没有完全管理权限的攻击者也可能提升权限控制服务器。漏洞可能带来服务器被完全控制、敏感数据被非法访问、恶意脚本和勒索软件被部署以及服务器被用作进一步攻击平台等严重后果。Webmin 官方已经发布 2.111 版本修复此漏洞，建议受影响用户及时升级

到安全版本。

65. Apache HugeGraph-Server 身份验证缺陷漏洞

漏洞编号　LDYVUL-2024-00842093 、 CVE-2024-43441
漏洞等级　严重
漏洞类型　身份验证缺陷
漏洞时间　2024-12-27 10:59:41

360 漏洞云监测到 Apache 软件基金会披露了一个影响 Apache HugeGraph-Server 的关键漏洞，此漏洞被评为 “严重” 级别，攻击者可利用假定不变的数据绕过认证机制，可能导致未经授权访问敏感图数据和操作。HugeGraph 团队已发布 1.5.0 版本进行修复，强烈建议 1.0 到 1.3 版本的用户立即升级到安全版本。此外，Apache HugeGraph-Server 在 2024 年 4 月还披露过另一个关键漏洞 CVE-2024-27348，该漏洞允许在存在漏洞版本的 Apache HugeGraph-Server 上实现远程代码执行，且存在在野利用。

四、 网络安全热点新闻

1. 微软称高管遭黑客组织攻击

1 月 19 日消息，一个威胁行为者窃取了微软高级领导团队成员以及网络安全和法律团队员工的电子邮件。此次攻击始于 2023 年 11 月底的密码喷射攻击，攻击者利用被攻破的账户权限访问了一小部分微软企业电子邮件账户并窃取了一些邮件和附件文档。微软表示其安全团队在 2024 年 1 月 12 日发现了攻击，并启动响应流程。目前调查仍在继续，微软称目前没有证据表明威胁行为者能够访问客户环境、生产系统、源代码或人工智能系统，且此次攻击不是微软产品或服务的漏洞导致。

2. 联邦调查局称已 “消除 ” 黑客对 SOHO 路由器的攻击

2 月 15 日消息，FBI 表示在 1 月份的行动中破坏了黑客对 Ubiquiti 的小型办公室 / 家庭办公室（SOHO）路由器的攻击活动。这是近期第二次披露破坏利用美国 SOHO 路由器的国家攻击行动。俄罗斯情报机构 GRU 的攻击利用默认管理员密码在 Ubiquiti Edge OS 路由器上安装恶意软件，将数百台路由器组成僵尸网络，用于对俄罗斯政府感兴趣的目标进行网络钓鱼和窃取凭证等活动，FBI 通过法院授权在 1 月将其破坏。同时，小公司可能认为自己不是国家攻击者的目标，但实际上越来越容易成为攻击对象。

3. Change Healthcare 数据泄露事件影响超过 1 亿人

2 月 20 日消息，Change Healthcare 发生数据泄露事件，影响超过 1 亿人，是美国有史以来最大的医疗保健数据泄露事件。2 月 21 日网络攻击扰乱其 IT 运营，超 100 个应用受影响，数千家药房和医疗服务提供商也被波及。该公司确认是由 ALPHV/Blackcat 实施的网络安全问题，正与执法部门及第三方顾问合作解决。被泄露数据包括多种个人信息。

4. ScreenConnect 工具中发现了高危漏洞 影响了云和本地实例

2 月 26 日消息，2024 年 2 月 13 日，ConnectWise 报告在其 ScreenConnect 工具中发现了漏洞，影响了云和本地实例。该公司通过 ConnectWise 信任中心通知了合作伙伴，2 月 19 日通知了 MSP，并指示他们立即更新本地服务器。ConnectWise 已经为所有云环境打了补丁，并且上周缓解了约 80% 的 ScreenConnect 用户问题，还为过去 20 个版本提供了回溯升级补丁。ConnectWise 的 CISO Patrick Beggs 强调保持良好网络卫生的重要性，总经理 Ciaran Chu 表示关键沟通对象是本地合作伙伴，公司每小时查看有多少本地合作伙伴在升级，并持续联系未升级的用户。

5. 网络犯罪团伙声称对医疗保健变革攻击事件负责

2 月 28 日消息,名为 Blackcat 和 Alphv 的网络犯罪组织宣称对 Change Healthcare 发动了网络攻击，并声称窃取了 6TB 的数据。UnitedHealth Group 的发言人表示公司已知晓此事并正在调查。此次攻击扰乱了美国的药店以及其他医疗设施和办公室。此前 UnitedHealth 将攻击归因于一个国家威胁行为者，如今 Blackcat 的宣称引发了质疑。Change Healthcare 周三的最新声明没有新信息，只是重复了之前的内容，称中断预计至少持续到当天，并正在采取多种方法恢复受影响的环境。UnitedHealth 周二表示，患者无法获取处方的报告很少，因为美国超过 90% 的药店被认为使用了“改进的电子索赔处理”来减轻影响。

6. CISA 和 Red Hat 就影响 Linux 发行版的供应链漏洞发出警告

3 月 29 日消息，Red Hat 和美国网络安全与基础设施安全局（CISA）警告称 XZ Utils 软件的两个最新版本（5.6.0 和 5.6.1）被植入了后门。XZ Utils 是一套广泛使用的数据压缩软件工具和库，几乎存在于每一个 Linux 发行版中。植入的代码可能允许恶意行为者突破安全外壳守护进程认证并远程获得对整个系统的未经授权访问。Red Hat 建议立即停止使用任何 Fedora Rawhide 实例，Fedora Rawhide 将很快恢复到 xz - 5.4.x 版本。CISA 建议开发者和用户将 XZ Utils 降级到未受影响的版本（如 XZ Utils 5.4.6 Stable），并寻找任何恶意活动并向 CISA 报告。

7. 美国电话电报公司调查影响 7000 多万客户的数据泄露事件

3 月 31 日消息，电信公司 AT&T 正在调查一起可能的数据泄露事件。超过 70 名当前和前客户的个人数据在暗网上被发现。AT&T 发表声明称大约两周前暗网上发布的数据集包含 AT&T 的特定数据字段，该数据集似乎来自 2019 年或更早，影响约 760 万当前账户持有者和约 6540 万前账户持有者。数据包括个人信息如社会安全号码等。目前尚不清楚数据是来自 AT&T 自身还是其供应商之一，公司已启动内部和外部专家支持的强大调查，主动与受影响者沟通并在适用情况下提供信用监测。

8. Ascension 网络攻击： 电子健康记录系统失灵，导致部分手术 ” 暂时中止 “

5 月 9 日消息，位于圣路易斯的阿森松医疗集团该集团遭受数据泄露，其电子健康记录系统不可用，一些非紧急的择期手术也暂停。集团表示正在与内部和外部顾问昼夜不停地工作以调查、控制并恢复系统。MyChart 系统、部分电话系统以及一些用于订购特定检查、程序和药物的系统也无法正常工作。患者被建议携带症状记录、当前药物清单等。阿森松集团有 13.4 万名员工、3.5 万名附属医疗服务提供者和 140 家医院。

9. Snowflake 客户在攻击中遭受 “重大” 数据盗窃：Mandiant

6 月 10 日消息，Mandiant 研究人员表示，一个网络犯罪集团涉嫌从 165 个组织窃取数据，其中针对 Snowflake 客户的攻击影响比之前认为的更广泛，有大量数据被盗，目前已知有 100 多个客户可能受到影响。受影响的账户未启用多因素身份验证，仅需用户名和密码即可成功认证。Mandiant 将攻击归咎于一个之前未知的、受经济利益驱动的威胁行为者 UNC5537，其利用窃取的客户凭证系统地攻击 Snowflake 客户实例，在网络犯罪论坛上出售受害者数据并试图勒索受害者。

10. CDK Global 在遭受两次网络攻击后关闭了大部分系统

6 月 20 日消息，CDK Global 是一家为数千家汽车经销商提供软件的供应商，在近日

遭受两次网络攻击后关闭了大部分系统。第一次攻击发生在周二，第二次攻击在周三。目前 CDK 正与第三方专家合作应对，这次攻击事件给依赖其软件的汽车经销商带来了诸多影响。

11. CocoaPods 的关键缺陷使 iOS 和 macOS 应用程序容易受到供应链攻击

7 月 1 日消息，E.V.A Information Security 研究人员在用于 Swift 和 Objective-C Cocoa 项目的 CocoaPods 依赖管理器中发现了三个安全漏洞，可能被用于发动软件供应链攻击，使下游客户面临严重风险。这些漏洞自 2023 年 10 月起已被 CocoaPods 修复，项目维护者也重置了所有用户会话。漏洞包括 CVE-2024-38368、CVE-2024-38366 和 CVE-2024-38367，其中 CVE-2024-38366 最为严重，可利用不安全的电子邮件验证工作流在 Trunk 服务器上运行任意代码。此外，通过欺骗 HTTP 标头可将漏洞升级为零点击账户接管攻击。

12. AT&T 数据泄露泄露了 1.09 亿用户信息

7 月 17 日消息，2024 年 4 月，AT&T 发生数据泄露事件，黑客获取了约 1.09 亿人的电话和短信记录。此次事件影响了 2022 年 5 月 1 日至 10 月 31 日以及 2023 年 1 月 2 日期间几乎所有移动客户。虽电话和短信内容未被获取，但包括了 AT&T 有线用户电话号码、联系的号码、通话或短信数量、特定日期或月份的通话时长等信息，部分记录还包括一个或多个小区站点 ID 号码。黑客可利用其他被盗数据库进行匹配，可能用于社会工程、在线冒充和网络钓鱼攻击。AT&T 将通过电子邮件或美国邮政联系受影响客户。此外，文章还提到了保护敏感数据的方法，如签订安全协议、加密敏感数据、定期审计等。

13. CrowdStrike 更新失误致全球 Windows 系统崩溃

7 月 19 日消息，全球网络安全领导者 CrowdStrike 出现重大问题，导致全球 Windows 系统宕机。受影响的主要领域包括金融、航空、医疗保健和其他关键服务提供商，造成广泛的运营中断。此次故障是由于 CrowdStrike 的 Falcon Sensor 安全软件的配置更新错误

引发的。该更新被识别为 Channel File 291，包含一个逻辑错误，导致软件驱动程序（CSagent.sys）发生越界内存读取，从而导致系统崩溃。受影响的 Windows 系统出现了臭名昭著的蓝屏死机。全球约有 850 万台微软 Windows 系统受到影响，导致航空、银行、医疗和紧急服务等关键行业出现广泛中断。此次事件导致的运营失败包括航班取消、支付处理问题和基本服务中断。

14. 法国奥运会期间遭遇超过 140 次网络攻击

8 月 14 日消息，在奥运会筹备期间及举办期间，法国网络安全机构一直处于高度戒备状态，以防范可能干扰奥运会组织委员会、票务系统或交通的攻击。7 月 26 日至 8 月 11 日期间，法国国家网络安全机构 Anssi 记录了 119 起低影响的“安全事件”报告以及 22 起“恶意行为者”成功攻击受害者信息系统的事件。攻击主要针对政府实体以及体育、交通和电信基础设施。

15. 疑似网络攻击导致西雅图机场陷入混乱

8 月 27 日消息，西雅图港在劳动节前夕疑似遭到网络攻击，严重扰乱了该市的机场和海运服务。8 月 24 日开始的 IT 中断导致西雅图 - 塔科马国际机场（SEA）的值机流程严重延误，目前没有 Wi-Fi，显示屏也无法正常工作。SEA 访客通行证和机场失物招领等某些机场程序和服务目前不可用。乘客被建议在到达机场前获取手机登机牌并托运行李以加快值机流程。边疆航空、精神航空、太阳乡村航空、捷蓝航空和国际航空公司受到的影响尤其大。西雅图港的网站目前无法访问，SEA 应用程序上也无法获取行李和航班信息。西雅图港的海运设施电话系统也因系统中断而无法使用，但游轮服务正常运行。此次事件影响了劳动节早期的旅行，美国劳动节为 9 月 2 日。运输安全管理局联邦安全总监强调旅行公众的安全未受影响，SEA 继续有效地对乘客和行李进行检查。当地政府机构于 8 月 24 日首次报告“互联网和网络系统中断”，随后表示某些系统的中断表明可能是网络攻击，并已隔离关键系统。

16. 全球首起通信设备武器化事件！黎巴嫩 BP 机爆炸致数千人死伤

9 月 17 日消息，黎巴嫩多地发生寻呼机爆炸事件，引发对网络安全的诸多思考。此事件造成多人伤亡，被指设备被以色列机构改装，可接收密码信息爆炸。这起事件引发全球对智能终端设备安全性担忧，打破网络世界和物理世界边界。强调供应链安全关乎国家安全，应警惕供应链攻击，从国家与行业监管、厂商和供应商、最终用户层面采取措施。同时指出联网风险激增，提升智能终端产品安全性势在必行，从创新技术、自主可控、产业生态层面着手。还提到网络战时代，亟需提升网络安全软硬实力，重视硬科技突破和软实力培养，构建全面网络安全防御体系。

17. 午夜暴雪使用 SDP 文件进行大规模鱼叉式网络钓鱼活动

10 月 21 日消息，自 2024 年 10 月 22 日起，微软威胁情报观察到 Midnight Blizzard 向政府、学术界、国防、非政府组织等领域的个人发送一系列高度针对性的鱼叉式网络钓鱼邮件。该活动使用包含指向攻击者控制服务器的签名远程桌面协议（RDP）配置文件的邮件，攻击了 100 多个组织的数千个目标。Midnight Blizzard 主要针对欧美等国家和地区的政府、外交实体、非政府组织和 IT 服务提供商，采用多种攻击方式获取目标设备访问权限以进行情报收集。微软为受影响的客户提供了缓解措施建议，并提供了检测、查询和威胁情报报告等资源。

18. 微软、Meta 和司法部瓦解全球网络犯罪和欺诈网络

11 月 22 日消息，Meta Platforms、Microsoft 和美国司法部（DoJ）宣布采取独立行动打击网络犯罪。Microsoft 的数字犯罪部门（DCU）查获了与埃及网络犯罪分子 Abanoub Nady 相关的 240 个欺诈网站，此人出售名为 ONNX 的网络钓鱼工具包，其犯罪活动可追溯至 2017 年。ONNX 以 “网络钓鱼即服务”（PhaaS）模式出售，价格每月 150 美元到六个月 550 美元不等，能绕过安全措施入侵微软客户账户，其身份被曝光后活动停止，该工具包也被美国金融行业监管局（FINRA）警告，Microsoft 获得法院命令以消除恶意技术基础设施。美国司法部宣布关闭 PopeyeTools 市场，该市场自 2016 年起出售被盗信用卡和金融欺诈工具，三名管理员被起诉，面临最高 10 年监禁，该市场估计出售了至少

22.7 万人的信息并获得至少 170 万美元收入。Meta 宣布关闭与柬埔寨、缅甸、老挝、阿联酋和菲律宾诈骗中心相关的 200 多万个账户，这些诈骗中心通过社交媒体平台和约会应用与全球目标建立关系进行诈骗，5 月 Meta 与 Coinbase、Ripple 和 Match Group 组成联盟对抗诈骗。

19. 360 发布全球首份《大模型安全漏洞报告》，曝光近 40 个大模型相关安全漏洞

11 月 26 日消息，全球人工智能浪潮下，大模型能力不断提升，但也带来新风险挑战。360 数字安全集团发布全球首份《大模型安全漏洞报告》，从模型层、框架层、应用层三大维度探查安全问题，审计发现近 40 个安全漏洞，影响众多知名框架和开源产品。报告指出大模型生成及应用过程存在隐忧，如被攻击可能导致服务不可用和安全损害；框架层安全边界模糊，攻击面增加，可能带来巨大损失；应用层安全中模块协同存在风险，可能致目标系统失控。360 数字安全集团打造安全大模型，遵循 “安全、向善、可信、可控” 原则，保障大模型服务安全运行，助力应对挑战，推动国内大模型生态持续健康发展。

20. 星巴克因供应商遭黑客攻击，被迫改用手写方式记录工资

11 月 27 日消息，星巴克的第三方软件供应商 Blue Yonder 遭勒索软件攻击，影响了星巴克员工排班和工时追踪系统。星巴克被迫采用手写方式记录工时和发放工资，虽门店营业未受影响，但仍在努力恢复系统功能。Blue Yonder 是松下子公司，客户涵盖多个行业，目前尚未给出问题解决时间表。此次事件也影响了部分英国超市连锁店，凸显了供应链攻击对企业运营的严重影响，企业应强化供应商管理、提升网络安全防护能力并建立应急备用方案，供应商也需构建漏洞管理体系。

21. TikTok 在最新安全举措中瞄准改变外观的滤镜和未成年人用户

11 月 28 日消息，TikTok 面临多方面挑战并采取相应措施。一方面，TikTok 因被指对青少年心理健康有影响在美国 14 个州面临诉讼，为此宣布限制 18 岁以下用户使用改变外貌的滤镜，并加强打击未成年用户使用平台。包括限制特定视觉效果、提供滤镜影响

信息以及更新创作者指南。另一方面，TikTok 为解决 13 岁以下用户使用平台问题，每月移除约六百万疑似未成年账户，并在英国测试新的机器学习系统以检测此类账户。限制滤镜和更新指南将在全球推出，但这些措施的效果尚不确定。此外，TikTok 还面临零日攻击以及因违反儿童在线隐私保护法面临民事诉讼。

22. 施乐、诺基亚、美国银行、摩根士丹利等公司 76 万员工的数据在网上泄露

12 月 2 日消息，施乐、诺基亚、科赫、美国银行、摩根士丹利等大型企业的数十万名员工成为去年 MOVEit 文件传输工具遭攻击引发的大规模数据泄露事件的最新受害者。一个名为 “Nam3L3ss” 的实体周一上午开始泄露这些公司及其他受影响公司员工的个人数据。2023 年 5 月与俄罗斯有联系的 Cl0p 勒索软件小组滥用 MOVEit 产品套件中的安全漏洞，导致数以千计的组织和数百万个人数据被访问。上个月 Nam3L3ss 已发布过亚马逊员工文件，本周又将其他大公司加入受害者名单。个人数据删除机构 Atlas Privacy 的首席战略官扎克·加诺特表示新泄露数据似乎真实，其运营的 databreach.com 可帮助人们检查和删除自己被泄露的数据。此次泄露包括超过 76 万名员工的详细信息，涉及多家大公司，但这些公司均未回应置评请求。加诺特称这些数据是社会工程学的 “金矿”。

23. 法国移动运营商联手应对日益猖獗的欺诈行为

12 月 3 日消息，法国四大主要移动网络运营商(MNOs)联手打击网络欺诈和身份盗窃。2025 年上半年将推出两个网络应用编程接口（APIs），此举措是全球移动通信系统协会（GSMA）开放网关计划的一部分。GSMA 成立于 1995 年，代表全球移动运营商利益，其开放网关计划于 2023 年启动，旨在促进数字产品设计。开发者可利用新的网络能力和 APIs 将服务接入。四大运营商提供的两个 APIs 为 KYC Match 和 SIM Swap，可帮助企业减少在线欺诈，未来还计划推出第三个 API——Number Verification。

24. 伏特加酒制造商 Stoli 在勒索软件攻击后在美国申请破产

12 月 3 日消息，Stoli 集团遭遇一系列重大危机。其美国公司在 8 月遭遇勒索软件攻击后申请破产，俄罗斯当局查封了该公司在俄剩余酿酒厂。攻击严重破坏了其 IT 系统，包括 ERP，导致手动操作和关键流程受影响，预计 2025 年初才能完全恢复。攻击还使美国子公司无法向贷款人提供财务报告。

25. GitLab 将停止对中国区用户提供 GitLab.com 账号服务

12 月 4 日消息，全球第二大开源代码托管平台 GitLab 宣布停止为中国大陆、澳门和香港的用户提供 GitLab.com 账号服务，推荐用户迁移至极狐。用户需在 2025 年 2 月 18 日前完成迁移，否则账户将被删除。GitLab 解释此决定是因其与极狐合作，极狐是其在中国的独家合作伙伴，能更好地服务中国区用户并专注本地化开发与支持。极狐于 2021 年成立，为中国市场提供独立运营的 GitLab DevOps 平台。虽然这一举措有助于推动本土化服务，但一些开发者认为迁移时间紧迫。极狐信息技术完全自主管理，确保平台本地化服务不断优化。GitLab 此举推动极狐本地化进程，为中国开发者提供更多本土 DevOps 解决方案，同时也引发部分用户吐槽迁移时间紧迫。

26. 欧洲刑警组织拆除了 15 个国家的 27 个 DDOS 攻击平台

12 月 12 日消息，全球执法行动 “PowerOFF” 成功打击了 27 个用于进行分布式拒绝服务（DDoS）攻击的压力测试服务，使其下线。此次行动由欧洲刑警组织协调，15 个国家参与，拆除了多个攻击网站，逮捕了相关管理员，并确定了 300 多名用户。发起此类攻击的动机多样，包括经济破坏、财务收益和意识形态原因等。美国司法部也对两名被告提出指控。参与 “PowerOFF” 行动的国家众多。此前德国也曾打击过相关犯罪服务，本月 Cloudflare 称美国购物和零售网站在购物季 DDoS 活动显著增加，同时还发现企业环境中存在可被利用进行 DDoS 攻击的漏洞，并给出了降低风险的建议。

27. 日本航空公司遭网络攻击导致全球瘫痪

12 月 30 日消息，日本航空公司（JAL）近期遭受重大网络攻击。此次攻击扰乱了航班运营，导致乘客延误，并引发了对航空业网络安全漏洞的担忧。日本航空是亚洲最著名的航空公司之一，以其广泛的全球网络和技术先进性而闻名。2024 年 12 月 26 日的攻击影响了航班预订、值机和行李处理等关键业务，造成乘客延误。航空公司虽确认了攻击，但未提供攻击者所用方法或攻击范围的具体细节。此次事件凸显了航空业网络安全的重要性，也引发了对该行业应对日益复杂网络威胁准备程度的质疑。目前，日本航空已采取紧急措施恢复正常运营。近年来，航空业频繁成为网络攻击目标，如易捷航空和印度航空也曾遭受攻击，这些事件表明航空公司面临的风险不断增加，急需加强网络安全措施。

28. 苹果公司将支付 9500 万美元解决 Siri 隐私诉讼

1 月 3 日消息，苹果同意支付 9500 万美元以解决一起集体诉讼。该诉讼称苹果的 Siri 语音功能侵犯用户隐私，会记录设备所有者的对话并与第三方分享。2019 年《卫报》报道引发此事，称苹果承包商 “经常” 收听录音，包括医生和患者等私密对话，且录音伴有用户数据。集体诉讼在报道一个月后提起，苹果否认有不当行为，称用户请求与 Apple ID 无关且有保密要求。原告称对 Siri 的陈述引发定向广告，苹果一直宣称重视隐私但被指用 Siri 模糊其隐私做法。根据和解协议，数千万集体成员每台支持 Siri 的设备可获得高达 20 美元赔偿。文章作者是报道隐私等内容的记者 Suzanne Smalley。

29. 日本最大移动运营商称网络攻击中断了部分服务

1 月 3 日消息，日本最大移动运营商 NTT Docomo 周四遭受网络攻击，部分服务中断后正努力恢复。此次攻击为分布式拒绝服务攻击（DDoS），导致其新闻网站、视频平台、移动支付、网络邮箱服务和高尔夫爱好者网站无法访问。2023 年该公司曾遭受勒索软件攻击。NTT Docomo 是近几个月来日本一系列网络攻击的目标公司之一。12 月日本航空公司部分航班因类似事件延误。上个月三井住友保险第三方供应商遭勒索软件攻击。去年有日本媒体公司向俄罗斯黑客支付赎金，10 月卡西欧因勒索软件攻击致交货延迟，还有其他多家日本公司及主要金融机构也遭受网络攻击。

五、 网络安全法规动态

1. 财政部印发《关于加强数据资产管理的指导意见》

1 月 11 日消息，财政部印发《关于加强数据资产管理的指导意见》（《资管意见》），涵盖总体要求、主要任务、实施保障三方面共十八条内容，目的在于释放公共数据价值，推动实体经济数字化转型与数字经济高质量发展。其明确了十二项主要任务，包括依法合规管理、明晰权责、完善标准、防范风险等，还提出通过加强组织实施、加大政策支持、鼓励试点来保障任务实施，且针对国有公共数据资产管理作出规定，为相关主体处理公共数据资产提供政策指导。

2. 中国电子信息行业联合会发布《数据合规审计指南》团体标准

2 月 18 日消息，中国电子信息行业联合会发布《数据合规审计指南》团体标准，《数据合规审计指南》以全面数据合规审计的鉴证业务为核心，为数据合规审计人员提供了执行标准，也为审计报告和结果的使用者提供了必要的参考信息，有助于构建数据合规与治理生态，促进数字经济健康发展。

3. 自然资源部发布《对外提供涉密测绘成果管理办法（征求意见稿）》

2 月 20 日消息，自然资源部发布《对外提供涉密测绘成果管理办法（征求意见稿）》，《对外提供涉密测绘成果管理办法（征求意见稿）》明确，对外提供涉密测绘成果应遵循维护国家安全和利益与满足对外交往合作相结合的原则，实行分级审批制度，由各级自然资源部门或部分省份的测绘地理信息局审批，审批前需征求军队测绘部门意见，必要时还可征求国务院、省级人民政府相关部门意见，生效后将规范新时期涉密测绘成果提供管理工作。

4. 中国银行业协会发布《银行业数据资产估值指南》

2 月 29 日消息，中国银行业协会发布《银行业数据资产估值指南》团体标准，通过明

确分类与估值方法，旨在为商业银行数据资产价值衡量问题予以指导。业内人士认为，这将有助于加速银行业探索数据要素市场化的步伐。

5. 国家标准委发布 GB/T 43697-2024《数据安全技术 数据分类分级规则》

3 月 21 日消息，《数据安全技术 数据分类分级规则》国家标准于 2024 年 10 月 1 日正式实施。该标准规定了数据分类分级的原则、框架、方法和流程，并给出重要数据识别指南，适用于各行业各领域、各地区、各部门及数据处理者开展数据分类分级工作。数据根据在经济社会发展中的重要程度以及遭泄露等情况对不同方面造成的危害程度，从高到低分为核心数据、重要数据、一般数据三个级别。核心数据主要包括关系国家安全重点领域、国民经济命脉等的数据；重要数据是特定领域等一旦泄露可能直接危害国家安全等的数据；一般数据是核心数据和重要数据之外的其他数据。

6. 联合国大会通过首个关于人工智能的全球决议

3 月 21 日消息，联合国大会于 3 月 21 日通过首个关于人工智能的全球决议。该决议具有 “里程碑意义”，呼吁推动开发 “安全、可靠和值得信赖的” 人工智能系统以促进可持续发展。决议强调制定人工智能系统标准，弥合数字鸿沟，实现可持续发展并应对全球挑战，特别是发展中国家的挑战。鼓励会员国和其他利益攸关方制定监管和治理办法及框架，采取行动与发展中国家合作并提供援助。强调在人工智能系统全生命周期内尊重、保护和增进人权和基本自由。鼓励以包容、公平、普惠方式开发人工智能系统并营造有利环境，同时强调数据管理的重要意义。决议认为需继续讨论人工智能治理领域发展动态，紧跟人工智能系统开发及应用步伐。

7. 国家网信办公布《促进和规范数据跨境流动规定》

3 月 22 日消息，国家互联网信息办公室公布《促进和规范数据跨境流动规定》，自公布之日起施行。《规定》对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度作出优化调整。《规定》明确了重要数据出境安全评估申报标准，提出

未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

8. 中央网络安全和信息化委员会办公室公布《网络暴力信息治理规定》

6 月 14 日消息，国家互联网信息办公室等部门公布《网络暴力信息治理规定》，对网络暴力信息治理提出多方面要求。包括明确网络暴力信息定义，要求网络信息服务提供者细化分类标准规则、建立特征库和样本库等加强识别监测；建立网络暴力信息预警模型；对存在风险的情况采取回应关切、限制流量等措施并及时报告；建立健全用户账号信用管理体系，进行真实身份信息认证；完善私信规则等保护用户权益；建立多部门协同工作机制进行有效监管。

9. 出于隐私考虑，巴西停止了 Meta 的人工智能数据处理

7 月 4 日消息，巴西数据保护机构 ANPD 暂时禁止 Meta 处理用户个人数据以训练其人工智能算法。理由包括处理个人数据基于不充分的法律假设、缺乏透明度、限制数据主体权利以及对儿童和青少年构成风险等。

10. 中央网信办启动“清朗•2024 年暑期未成年人网络环境整治”专项行动

7 月 13 日消息，2024 年 7 月中旬以来，中央网信办深入开展 “清朗·2024 年暑期未成年人网络环境整治” 专项行动，全面覆盖直播、短视频、社交、电商等重点环节，集中整治危害未成年人身心健康的突出问题。专项行动期间，累计清理拦截涉未成年人违法不良信息 430 万余条，处置账号 13 万余个，关闭下架网站平台 2000 余个。中央网信办还通报了部分典型处置案例，网信部门将持续深化专项行动治理成效，督促网站平台履行未成年人网络保护主体责任，对问题突出、整改不力的平台和账号依法从严处置处罚。

11. 国家网信办就《人工智能生成合成内容标识办法（征求意见稿）》公开征求意见

9 月 14 日消息，国家互联网信息办公室发布《人工智能生成合成内容标识办法（征求意见稿）》及配套国家标准《网络安全技术 人工智能生成合成内容标识方法（征求意见稿）》，旨在规范人工智能生成合成内容标识，促进人工智能健康发展，保护合法权益与维护社会公共利益。文章介绍了该办法的主要内容，包括明确适用对象与范围、区分标识类型与使用场景及部署方式、新增网络信息内容传播平台服务提供者的核验与标识义务、新增用户获取不含显式标识内容的前提要件与标识义务等，同时也指出办法中有待明确的问题，期待其在完善过程中为公众带来更好的人工智能应用环境。

12. 国务院公布《网络数据安全管理条例》

9 月 30 日消息，《网络数据安全管理条例》公布，该管理条例旨在规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。

13. 欧盟发布《人工智能法案》，为人工智能引入一个共同的监管和法律框架

10 月 8 日消息，2024 年 8 月 1 日，欧盟《人工智能法案》正式启动，对欧洲人工智能的监管方式带来重大变革。该法案旨在平衡人工智能创新与安全公平，涵盖了法案内容、影响对象、风险类别、关键期限以及对不同组织的影响等方面。

14. 美国政府发布《联邦零信任数据安全指南》

11 月 1 日消息，由美国联邦首席数据官（CDO）委员会和联邦首席信息安全官（CISO）委员会联合牵头，联邦政府 IT 领导层在 10 月 31 日发布《联邦零信任数据安全指南》，旨在强化数据安全实践。这份文件共 42 页，重点强调了“保护数据本身，而非保护数据的

边界”。官方认为这一理念是“有效实施零信任的基础支柱”之一。

15. 德国联邦司法部发布计算机刑法草案，白帽黑客迎来合法曙光

11 月 8 日消息，德国联邦司法部发布计算机刑法草案，为白帽黑客提供法律保障。明确网络安全研究人员在发现并报告软件漏洞时不承担刑事责任，为全球安全研究人员树立法律标杆。现有的德国《刑法》使善意安全研究人员可能因访问漏洞系统面临刑事责任，此次草案旨在修复法律盲区。草案主要内容包括明确白帽黑客合法地位、规定漏洞披露合法途径、增强跨境合作以及设立合规与奖励机制。该草案标志着德国网络安全领域的重要法律变革，为全球网络安全法律框架提供借鉴，有助于构建更安全可信的数字化未来。

16. 美国会拟立法：小微企业实施网络安全合规可抵免税费

11 月 25 日消息，美国国会山的立法草案将给予一些小型企业税收抵免，以帮助其支付遵守国防部即将实施的网络安全成熟度模型认证（CMMC）计划的成本。该立法旨在解决长期以来的担忧，即 CMMC 合规成本将迫使小型企业退出国防业务。草案名为 “2024 年小企业网络安全法案”，允许员工不超过 50 人的公司为 CMMC 成本申请最高 5 万美元的税收抵免，由众议员斯科特·菲茨杰拉德（R--Wis.）发起。税收抵免可用于支付 CMMC 评估费用以及解决评估中发现的网络安全差距的费用。该法案不太可能进入 2025 财年国防授权法案，但可能在明年共和党讨论的减税延期中出现，不过其前景不确定，因为国防部尚未开始实施 CMMC 认证计划。CMMC 计划已筹备多年，国防部预计明年开始在合同中纳入要求，尽管进行了简化和精简，小型企业仍担忧成本问题，国防部支持税收激励措施，草案聚焦员工少于 50 人的公司，旨在平衡成本与财政限制。

17. 澳大利亚通过法案 16 岁以下禁用社交媒体

11 月 28 日消息，澳大利亚联邦议会参议院于 11 月 28 日通过《2024 网络安全（社交媒体最低年龄）修正案》，禁止 16 岁以下未成年人使用多数社交媒体平台，此前众议院已通过该法案。相关规定将在 12 个月后生效，脸书、X、照片墙等平台预计将受影响。若社交媒体公司未阻止 16 岁以下未成年人使用其平台，最高将被罚款 5000 万澳元，而

未成年人及其父母不会受罚。同时，公司不能强迫用户提供政府身份证件。澳大利亚总理阿尔巴尼斯表示社交媒体虽有社会效益，但也带来社会危害，可能成为霸凌、焦虑的来源和网络罪犯的工具，年轻人面临风险最大。

18. 特朗普网安政策重大转向：CISA 收缩，减少监管

12 月 24 日消息，美国网络安全与基础设施安全局（CISA）在不同政治环境下的发展变化。CISA 在特朗普第一个任期成立，起初任务是非政治性的，负责协调防御美国基础设施免受网络攻击并分享关键信息。但 2020 年选举后，CISA 因打击“错误信息”引发保守派反弹。克里斯·克雷布斯因拒绝特朗普政府的欺诈指控被解雇，詹·伊斯特利接任后采取低调方式，仍遭保守派不满。拜登执政期间，CISA 积极发展，取得了一些成就，但也面临批评。2024 年选举后，伊斯特利将辞职，CISA 未来在特朗普政府下可能面临角色缩减，同时也可能为私营部门带来新机会。

19. 土耳其出台更严格的加密货币反洗钱法规

12 月 25 日消息，2024 年最后一周，土耳其受世界主要司法管辖区（包括欧洲）积极的监管发展启发，推出了新的加密货币法规。新法规规定，交易额超过 15000 土耳其里拉（425 美元）的用户需向加密服务提供商提供身份信息，旨在防止通过加密货币交易洗钱和资助恐怖主义。该法规将于 2025 年 2 月 25 日生效，届时服务提供商还需收集未注册钱包地址用户的信息，若无法获取必要信息，交易可能被视为“有风险”，服务提供商可考虑暂停。2024 年土耳其加密公司活动增加，截至 8 月，土耳其资本市场委员会收到 47 份加密公司许可证申请。土耳其允许个人购买、持有和交易加密货币，但自 2021 年起禁止用于支付，目前不征收加密货币利润税，但在考虑征收 0.03% 的交易税。

20. 经过五年谈判，联合国大会通过网络犯罪公约

12 月 26 日消息，联合国大会于周二通过了具有里程碑意义的网络犯罪公约，为各国政府监管互联网的方式带来重大变革。该公约经过五年谈判以协商一致方式通过，2025 年将在河内举行正式签署仪式，批准后 90 天生效。公约为不同国家执法机构在网络犯罪调

查方面的协调提供了框架，但人权活动家、网络安全专家和一些大型科技公司表示反对，担心被独裁政权滥用并可能导致一系列隐私侵犯。美国和英国决定支持俄罗斯提出的这项措施，美国官员表示将要求滥用条约的政府承担责任。尽管存在担忧，但该公约仍被认为将在预防和打击网络犯罪、保护人们在线权利方面发挥关键作用。

六、 漏洞云情报服务介绍

为响应国家各级监管机构关于各单位对外部的漏洞开展快速响应和处置的工作要求，深化推进行业安全体系建设，360 漏洞云情报平台为客户提供定制化的漏洞情报推送及监测服务，服务特点如下：

多源整合，数据全面：1W+监测点，涵盖 CNVD、CNNVD、NVD 等权威漏洞库，24 小时不间断监测全球网站、博客、Twitter 等信息平台的安全漏洞资讯。自有 360BugCloud 开源漏洞收集平台、360 漏洞研究院可以持续产出高价值独家战略级零日漏洞情报。目前已储备标准化漏洞数量 30W+。

多渠道推送，及时响应：通过大数据、全天候、分布式的漏洞情报智能分发平台，漏洞情报可以通过邮件、微信消息或 API 接口的方式，助力漏洞情报推送极速响应，实现对企业客户多维触达，让企业走在安全的最前沿。

精准检测，方便验证：通过漏洞专家团队赋能，用标准化 POC 脚本实现漏洞的批量检测，快速精准发现企业内部资产存在的漏洞威胁。情报中机读关联信息可与客户业务联动，将企业 IT 资产与漏洞情报进行智能匹配分析，锁定受影响资产，辅助企业快速定位漏洞，确认危害等级。

专业补丁，助力漏洞修复：依托于 360 安全大脑强大的数据支撑，结合 360 漏洞云、漏洞研究院资深专家的漏洞分析研判，第一时间为企业提供漏洞防护策略及相应补丁，为客户抢占漏洞处置时机，消除漏洞隐患。

建议您订阅 360 漏洞云-漏洞情报服务，获取更多漏洞情报详情以及处置建议，让您的企业远离漏洞威胁。

联系电话：010-52447660

邮箱地址：g-ldyvi@360.cn

官网地址：https://vi.loudongyun.360.net

360 数字安全集团(三六零数字安全科技集团有限公司)是数字安全的领导者，以“上山下海助小微”为战略方向，专注为国家、城市、大型企业、中小微企业提供数字安全服务。过去 18 年，360 投入 250 亿，聚集超 2000 名安全专家，积累了 2000PB 安全大数据，为数字经济、数字政府、数字社会的建设提供全方位的安全解决方案，帮助城市、政府、企业规划和建设数字安全体系，形成应对数字安全复杂威胁的完整能力。

https://360.net