2022 上半年漏洞威胁分析报告

目 录

引言

回顾 2022 上半年，国际形势严峻，网络攻击事件频发。一方面，受 2021 年底的 Apache Log4j 重大漏洞影响，Log4j 系列漏洞在网络攻击中频繁被使用；另一方面，在国际形势的影响下，网络攻击较往年更为频繁。本报告从漏洞披露和漏洞攻击两个角度来分析 2022 上半年的漏洞态势，得出如下结论：开源软件的安全性逐渐引起重视；Nday 漏洞利用形势严峻，侧面反映出人员的安全意识不足；企业、政府、教育类行业更易遭受到攻击。

一、信息安全漏洞基本情况

1.1 漏洞总体情况

截止 2022 年 6 月底，NVD 漏洞库收录 2022 年的漏洞信息共 12347 条，相较于去年同期的 9432 条有了大幅提升。NVD 漏洞库历年数据统计如图 1 所示，可以看出漏洞数量整体呈增长趋势， 2017 年出现了爆发式增长，此后每年数量一直呈现上升趋势。

图 1　NVD 漏洞库 2001 年-2022 上半年漏洞数量统计

1.2 漏洞危害等级

根据 CVSS2.0 评分标准，将漏洞危害等级划分为低危、中危、高危三种，其反映了漏洞利用的难易程度及影响程度。统计 NVD 漏洞库历年漏洞危害等级占比情况如图 2 所示，可以看出高危漏洞的占比整体呈现下降趋势，中危漏洞占比呈现上升趋势，低危漏洞占比变化不大。

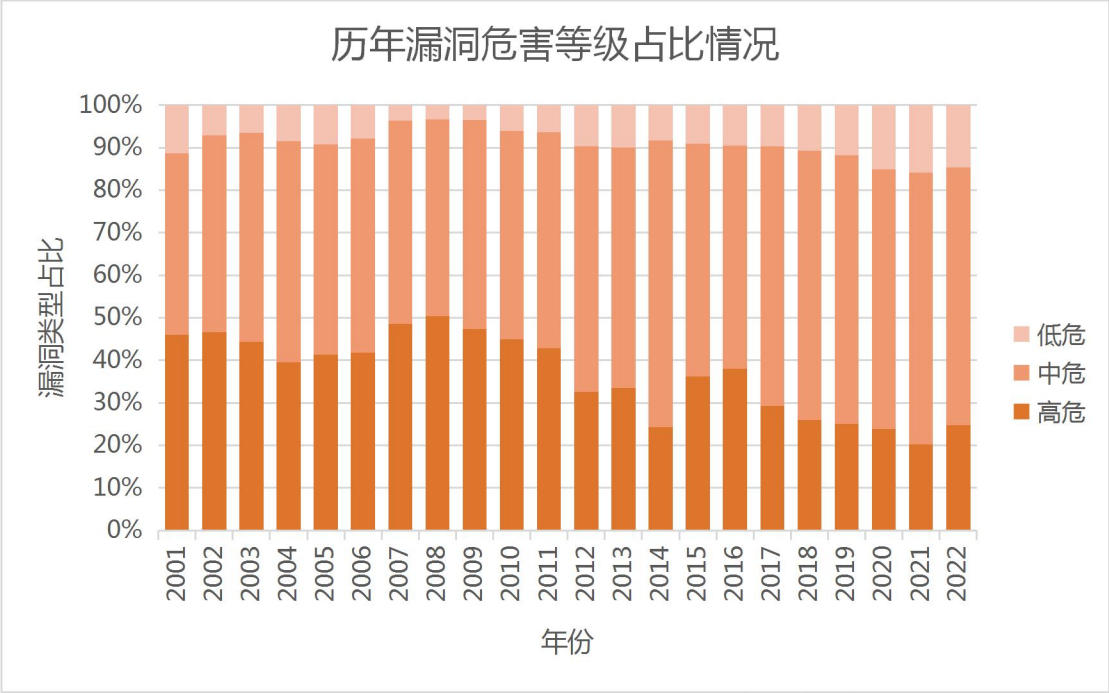


图 2　NVD 漏洞库 2001 年-2022 上半年漏洞危害等级占比情况

1.3 漏洞类型分布情况

根据威胁类型，将漏洞分为不同漏洞类型，统计 NVD 漏洞库历年漏洞类型占比如图 3 所示，可以看出，XSS 攻击和缓冲区错误两类漏洞一直都占有很高的比例，这表明他们通常比较容易发现和利用，在日常防护中要加强此类漏洞的防护。

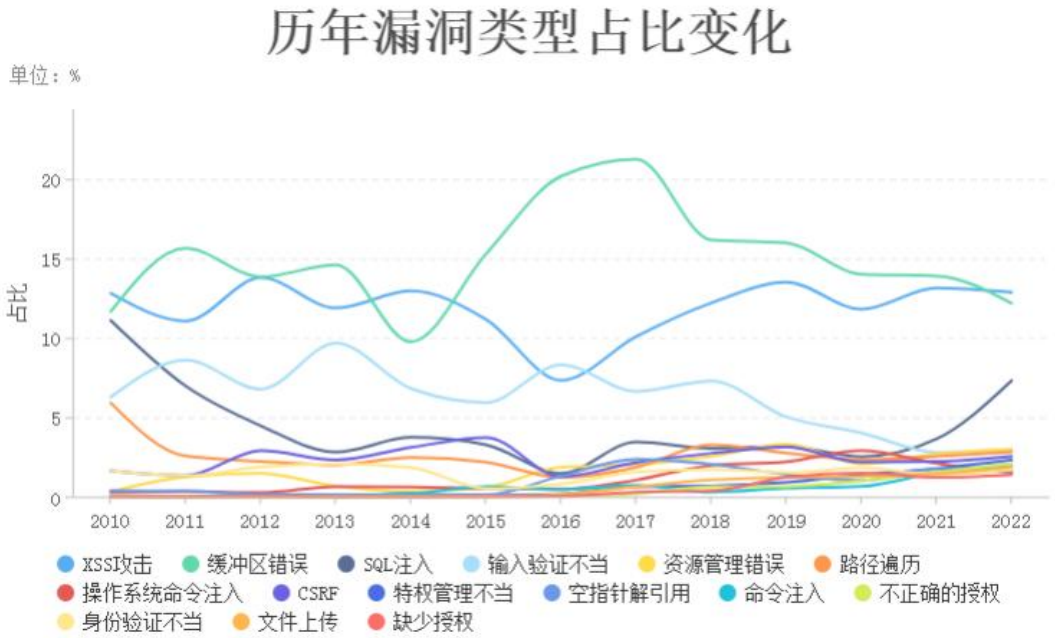


图 3　NVD 漏洞库 2010 年-2022 上半年漏洞类型占比情况

1.4 漏洞影响厂商

根据漏洞影响厂商进行分类，统计 NVD 漏洞库中近三年的漏洞数据，影响厂商情况如图 4 所示，其中漏洞数量较高的厂商有：Microsoft、Google、Apple、Oracle、Adobe、Linux 等。Microsoft、Apple、Oracle 等因其会固定时间发布安全补丁，所以其漏洞的数量较多。此外，由于开源软件越来越多地被使用，其漏洞数量也在逐年增高，如 Linux、IBM、Apache 等。

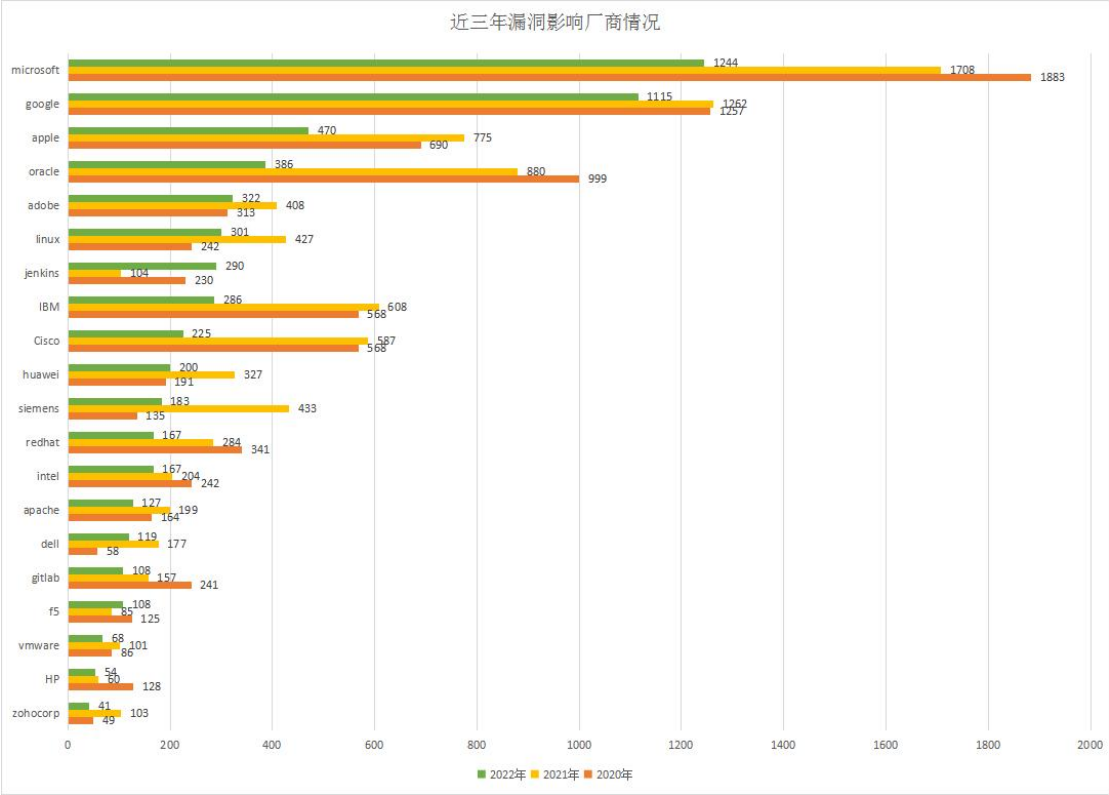


图 4　NVD 漏洞库近三年漏洞影响厂商分布情况

二、漏洞攻击情况

2.1 漏洞利用情况

根据 Palo Alto 的 Unit42 最新发布的《2022 年事件响应报告》，2022 年上半年被利用最多的漏洞是“ProxyShell”利用链，占记录的漏洞利用事件总数的 55%。ProxyShell 是一种组合利用三个漏洞（CVE-2021-34473、CVE-2021-34523 和 CVE-2021-31207）的攻击。Log4Shell 紧随其后，占 14%，如图 5 所示。这一数据与美国 CISA 发布的 2021 年最常被利用的漏洞高度重合，如表 1 所示。这说明陈旧漏洞一直在被重复利用，因为其利用的复杂度低、影响高，但根本原因是用户没有及时更新补丁，导致攻击者有机可乘。

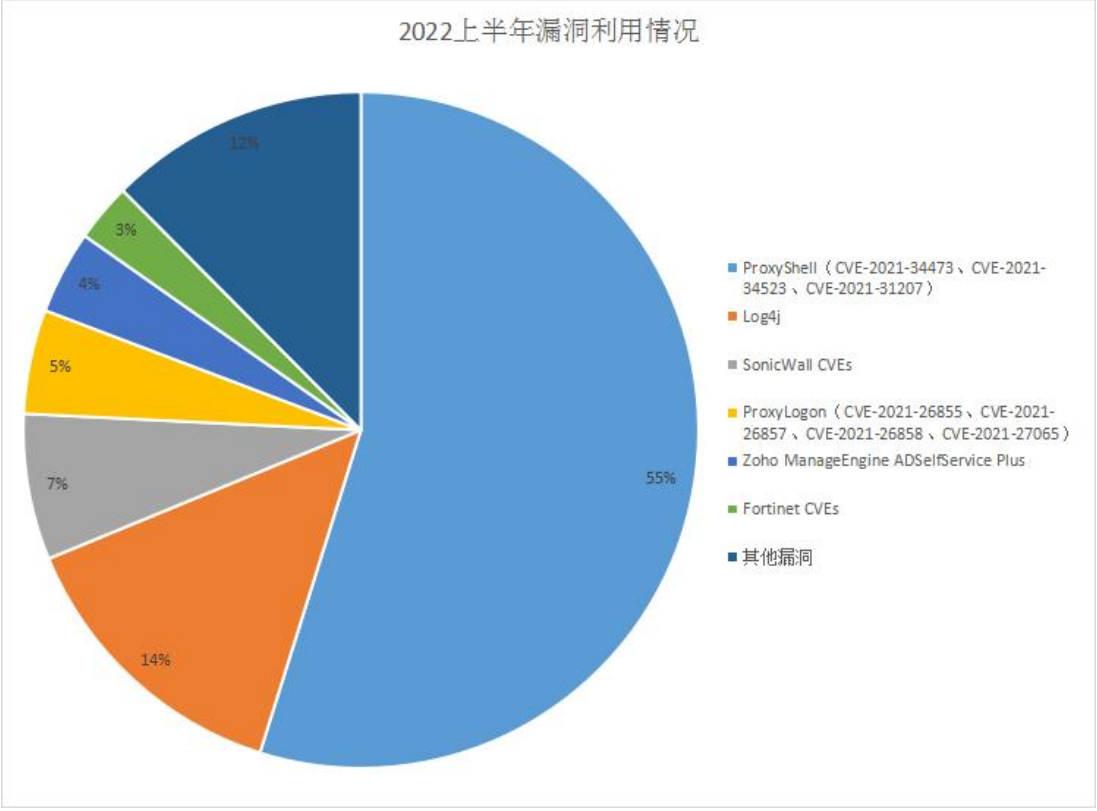


图 5　2022 上半年漏洞利用情况

表 1　2021 年最常被利用漏洞情况

厂商	CVE 编号	漏洞类型
Apache	CVE-2021-44228	远程代码执行
Zoho	CVE-2021-40539	远程代码执行
Microsoft	CVE-2021-34523	权限提升
Microsoft	CVE-2021-34473	远程代码执行
Microsoft	CVE-2021-31207	安全功能绕过
Microsoft	CVE-2021-27065	远程代码执行
Microsoft	CVE-2021-26858	远程代码执行
Microsoft	CVE-2021-26857	远程代码执行
Microsoft	CVE-2021-26855	远程代码执行
Atlassian	CVE-2021-26084	任意代码执行
VMware	CVE-2021-21972	远程代码执行
Microsoft	CVE-2020-1472	权限提升
Microsoft	CVE-2020-0688	远程代码执行
Pulse	CVE-2019-11510	任意文件读取
Fortinet	CVE-2018-13379	目录遍历

2.2 漏洞攻击行业分布

根据深信服云端监测的漏洞规则拦截数据，按照行业划分，其中常被漏洞攻击的行业是企业，占比 48.85%，其次是政府、教育，分别占比 18.38%和 13.11%，如图 6 所示。

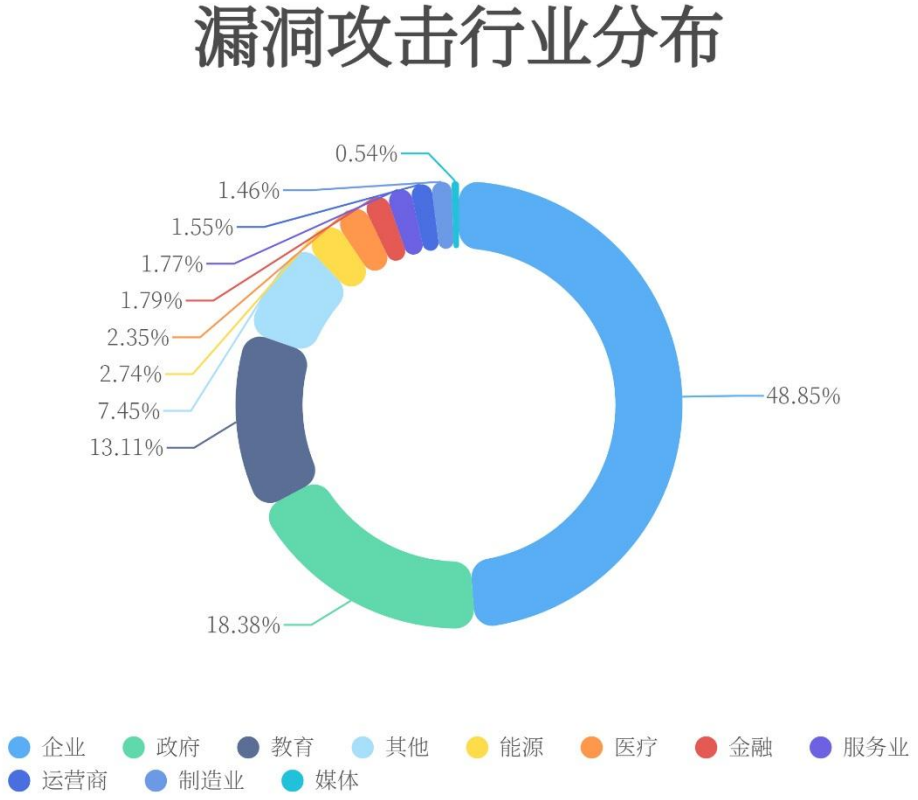


图 6　2022 上半年漏洞攻击行业分布情况

2.3 漏洞攻击省份分布

根据深信服云端监测的漏洞规则拦截数据，按照漏洞攻击省份划分，其中被攻击次数最多的省份是北京市，达到了两亿余次，其次是广东省、内蒙古自治区，数量都超过了一亿次，如下图所示。

漏洞攻击省份分布图

图 7　2022 上半年漏洞攻击地域分布情况

三、漏洞态势总结

3.1 开源软件安全引起重视

自去年的 Apache Log4j 漏洞后，开源软件安全引起行业内极高的重视。从近三年的 NVD 漏洞库中影响的厂商产品数量变化可以看出，开源软件的漏洞每年都在增长，如：Linux 从 2020 年的 242 个到 2021 年的 427 个再到今年上半年的 301 个，Apache 从 2020 年的 164 个到 2021 年的 199 个再到今年上半年的 127 个。因为开源软件的非商业性，开发人员的安全意识不高，也没有多余预算对其进行安全性测试，且攻击成功后的影响范围更广，导致黑客攻击的目标逐渐转移至开源软件，开源软件的安全也引起更多的重视。

3.2 Nday 漏洞利用形势严峻，安全意识亟需提高

对比 2021 年和 2022 上半年最常被利用的漏洞，发现其具有高度重合性。2022 上半年被利用的漏洞中，绝大部分是 2021 年披露的，有一部分甚至更早。这些漏洞仍然能被攻击者利用发起攻击，说明安全意识的不足，没有及时修补漏洞，导致 Nday 漏洞依然是黑客手中的利器。一旦 Nday 漏洞没有及时被修复，那么将会成为大规模杀伤性武器。因此，提升人员的安全意识、及时修补漏洞变得尤为重要和紧迫。

3.3 企业、政府、教育类行业更易遭受到攻击

今年上半年，在深信服云端监测到的漏洞攻击中，针对企业的攻击占 48.85%，针对政府的攻击占 18.38%，针对教育的攻击占

13.11%。勒索组织通常会向企业发起攻击，以获取更高的赎金，APT组织会向政府、教育行业发起攻击，获取机密且有价值的信息，而这两类攻击在初始阶段通常会选择利用漏洞来打开缺口。也因此，企业、政府、教育类行业一直是网络攻击的重灾区，做好这方面的防护已经刻不容缓。

四、附录-2022 上半年重大安全漏洞事件

1. Spring 框架存在远程命令执行漏洞(CVE-2022-22963)

Spring Cloud Function 是美国 Pivotal 公司的 Spring 团队的一个子项目，该项目提供了一个通用的模型，用于在各种平台上部署基于函数的软件。

该漏洞是由于 Spring Cloud Function 未对 HTTP 请求头部数据进行有效的验证，攻击者可利用该漏洞构造恶意数据进行远程代码执行，最终控制目标服务器。

影响范围：3.0.0≤Spring Cloud Function≤3.2.2

2. F5 BIG-IP iControl REST 身份验证绕过漏洞(CVE-2022-1388)

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。

该漏洞是由于 iControl REST 的身份验证功能存在缺陷，攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行身份验证绕过攻击，最终接管设备控制平台。

影响范围：16.1.0 ≤ F5 BIG-IP ≤ 16.1.2

15.1.0 ≤ F5 BIG-IP ≤ 15.1.5

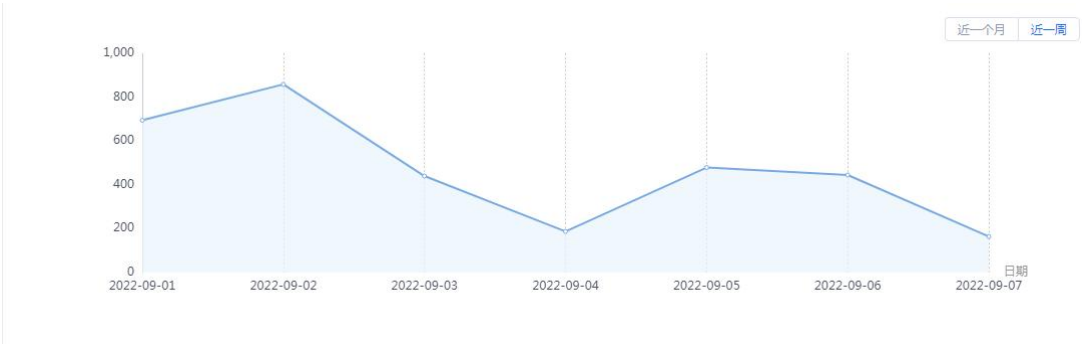
14.1.0 ≤ F5 BIG-IP ≤ 14.1.4

13.1.0 ≤ F5 BIG-IP ≤ 13.1.4

12.1.0 ≤ F5 BIG-IP ≤ 12.1.6

11.6.1 ≤ F5 BIG-IP ≤ 11.6.5

近一周攻击活跃趋势：



3. Atlassian Confluence Server and Data Center 远程代码执行漏洞（CVE-2022-26134）

Atlassian Confluence Server and Data Center 是澳大利亚 Atlassian 公司的一套专业的企业知识管理与协同软件，也可以用于构建企业 WiKi。该软件可实现团队成员之间的协作和知识共享。

该漏洞是由于数据处理不当，攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行 OGNL 表达式注入攻击，最终导致远程代码执行。

影响范围：Atlassian Confluence Server and Data Center < 7.4.17

7.5.0 ≤ Atlassian Confluence Server and Data Center < 7.13.7

7.14.0 ≤ Atlassian Confluence Server and Data Center < 7.14.3

7.15.0 ≤ Atlassian Confluence Server and Data Center < 7.15.2

7.16.0 ≤ Atlassian Confluence Server and Data Center < 7.16.4

7.17.0 ≤ Atlassian Confluence Server and Data Center < 7.17.4

7.18.0 ≤ Atlassian Confluence Server and Data Center < 7.18.1

五、了解更多

深信服千里目安全技术中心持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全技术中心掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全技术中心微信公众号，第一时间了解更多漏洞情报。