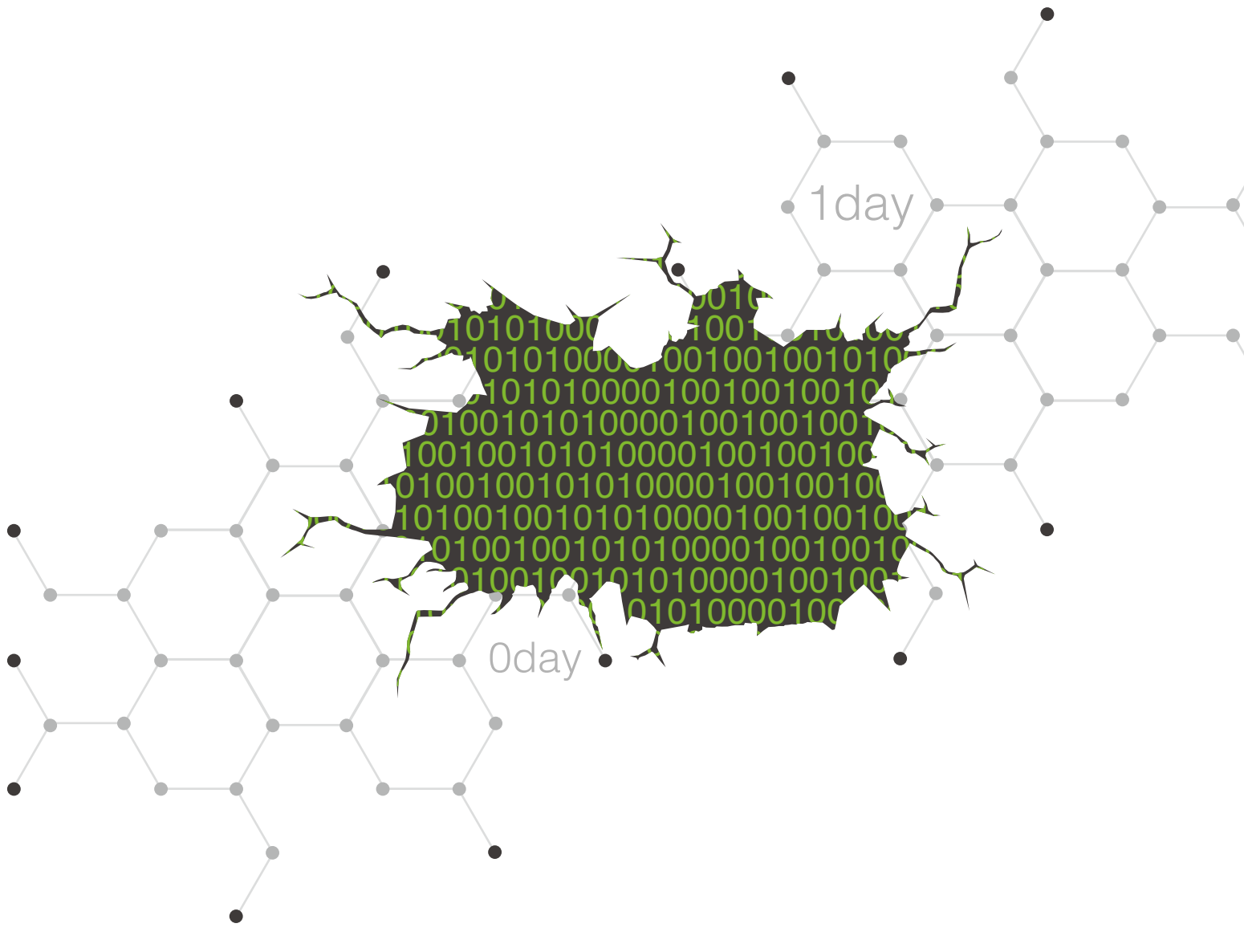
# 漏洞发展趋势

NSFOCUS

天机实验室
NSFOCUSTIANJI LAB



## 关于绿盟科技

绿盟科技集团股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市，证券代码：300369。绿盟科技在国内设有 40 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡设立海外子公司，深入开展全球业务，打造全球网络安全行业的中国品牌。

# 目录

摘要 ····· 2
1. 历史漏洞回顾 ····· 4
1.1 漏洞数量逐年显著增长 ····· 5
1.2 通用软件产品的漏洞数量排名 ····· 8
1.2.1 操作系统漏洞排名 ····· 8
1.2.2 应用软件漏洞排名 ····· 9
2. 漏洞利用情况 ····· 11
2.1 典型漏洞攻击事件监测举例 ····· 12
2.2 实际攻击中常用到 Nday 漏洞 ····· 14
3. 漏洞发展趋势 ····· 16
3.1 浏览器漏洞种类复杂多样 ····· 17
3.2 文档类型漏洞是鱼叉攻击的重要载体 ····· 19
3.3 Flash 漏洞面临消亡 ····· 21
3.4 开源软件面临漏洞利用和软件供应链的双重攻击 ····· 22
3.5 Android 和 iOS 漏洞加剧移动安全的威胁 ····· 24
3.6 安全堪忧的 IoT 设备 ····· 26
4. 结论 ····· 28

# 摘要

随着计算机网络技术的发展，全球互联网体量急速膨胀，网络安全形势日益严峻，国家政治、经济、文化、社会及公民在网络空间的合法权益面临严峻挑战。近些年来安全漏洞数量呈现递增趋势，基于漏洞的网络安全事件层出不穷，为我们敲响了信息安全攻防战的警钟。

软件由于开发及设计等各方面的原因，存在漏洞在所难免。对安全研究人员来说，通过对漏洞发展趋势的研究，可以在攻击者利用漏洞造成危害之前，提出及时有效的修补方案，尽可能的减少攻击事件的发生。对软件开发商来说，通过对漏洞的研究，可以帮助开发人员把更多的精力放在安全开发过程中需要注意的关键技术上，开发出高质量的软件。本文以 NVD 为数据源 [1]，对截止 2019 年底的历史漏洞数据进行分析总结，并基于绿盟威胁情报中心 (NTI)，得出以下观点：

1. 通过对历史漏洞数据的回顾，可以看到漏洞数量呈现显著增长的总体趋势，2019 年的漏洞数量比 1999 年增长了 9.62 倍。
2. 操作系统被公开的漏洞中，开源操作系统占比相对更高，其安全性问题可能暴露的更充分。如排名第一的 Debian Linux 系统在过去的 20 年累计发现了 3705 条漏洞，以高效快速地修复安全问题著称。
3. 根据绿盟威胁情报中心显示，十年以上高龄漏洞在攻击事件中占比仍然高，对于这些历史悠久的漏洞，由于攻击门槛低，攻击者依然在大量使用。
4. 浏览器作为网络攻击的入口，漏洞种类复杂多样。通过对应用类软件漏洞利用在网络攻击事件进行统计，浏览器漏洞利用占比 48.44%，影响范围广，安全人员仍需关注浏览器的更新与防护。
5. 利用文件格式漏洞的鱼叉式钓鱼攻击已成为网络安全的主要威胁之一，攻击者通过诱导目标对象点击打开包含漏洞的 PDF 或者 Office 文档，继而执行文档中内嵌的恶意脚本，此类漏洞利用稳定性高，在 APT 攻击事件中屡见不鲜。
6. Flash 漏洞作为曾经的研究焦点，2015 和 2016 年爆出的漏洞总数占据 Flash 漏洞的 55.09%。

1 NVD 数据库是国际主流数据库之一，其以 CVE 条目的信息为基础，提供更多增强版信息和公开查阅接口，本文全部采用 NVD 数据库数据进行统计计算。

在实际攻击中常以插件形式被嵌套在各种 Exploit Kit 工具包，可以达到稳定利用，更新速度快以及免杀的效果。今后一段时间内，Flash 漏洞并不会彻底消亡，还需继续关注。

7. 开源软件便于研究员进行基于源代码的白盒测试。Web 类开源框架的利用代码公开后可以在短时间内被集成到成熟的攻击框架中，降低了漏洞利用的门槛。随着开源软件开发模式的兴起，针对软件供应链的攻击成为面向软件开发人员和供应商的一种新兴威胁。
8. 移动设备的安全决定着家庭和企业用户的信息资产的安全。近些年来社会各界对移动应用的漏洞关注度逐渐提高，漏洞的产生不仅带来用户设备与信息的安全影响，也给企业带来业务或声誉上的损失。
9. 物联网设备数量增长迅速，大部分存在默认账户和弱口令，且大部分漏洞利用简单，攻击者容易构建僵尸网络，存在极大的安全风险，设备厂商应该重视并加强自身产品的安全。

# 1

# 历史漏洞回顾

# 1.1 漏洞数量逐年显著增长

截至2019年底，NVD数据库共收录漏洞信息138909条，历年漏洞的数量及同比增长率如图1.1所示。从 2005 年之后漏洞数量显著提升，同比增长 137%，2016 年更是突破万数大关，同比增长 411%，呈现快速增长的趋势。

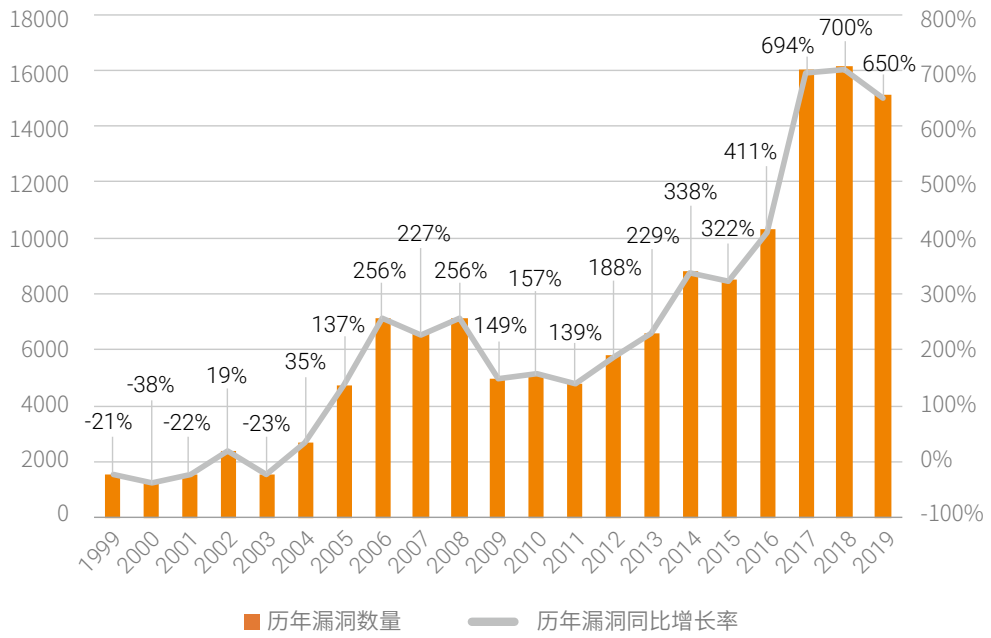



图 1.1 历年漏洞数量统计

为了更准确的表示漏洞环境所面临的风险，行业给出了一套通用漏洞评分系统 CVSS(Common Vulnerability Scoring System)，用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度。由于 CVSS v3.0 标准在漏洞覆盖率上不足，下文分析采用 CVSS v2.0 标准进行，其划分漏洞等级如表 1.1 所示。

表 1.1 CVSS v2.0 标准

| 等级 | CVSS 分数 |
|---|---|
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-10.0 |

## 历史漏洞回顾

根据 CVSS v2.0 等级标准，7.0-10.0 为高危漏洞，4.0-6.9 为中危漏洞，0.1-3.9 的则为低危漏洞。截止 2019 年底共有 130937 条漏洞分配了 CVSS v2.0 等级，各个等级按数量分布的占比如图 1.2 所示。

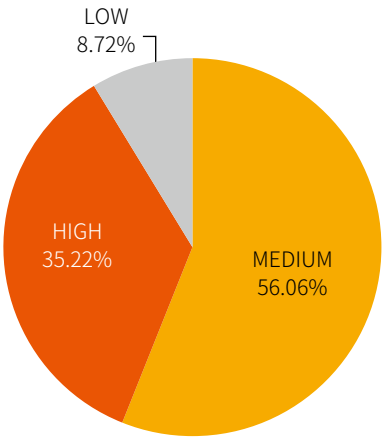



图 1.2 漏洞的 CVSS V2.0 分布

低危漏洞占据漏洞总数的 8.72%，攻击者利用此类漏洞可以获取某些系统或服务的信息、读取系统文件和数据。中危漏洞占 56.06%，攻击者利用此类漏洞可以远程修改、创建、删除文件或数据，或对普通服务进行拒绝服务攻击。高危漏洞占据 35.22%，攻击者利用此类漏洞可以远程执行任意命令或者代码，有些漏洞甚至无需交互就可以达到远程代码执行的效果。

NVD 数据库提供 CWE 条目，可对漏洞成因进行统一的分析。本文所分析的 138909 条漏洞中，共有 130961 条分配了 CWE ID。图 1.3 给出了 TOP20 CWE 漏洞类型 [1]。

1 该排名不包含 NVD-CWE-noinfo（信息不足）和 NVD-CWE-Other（其他）的数据

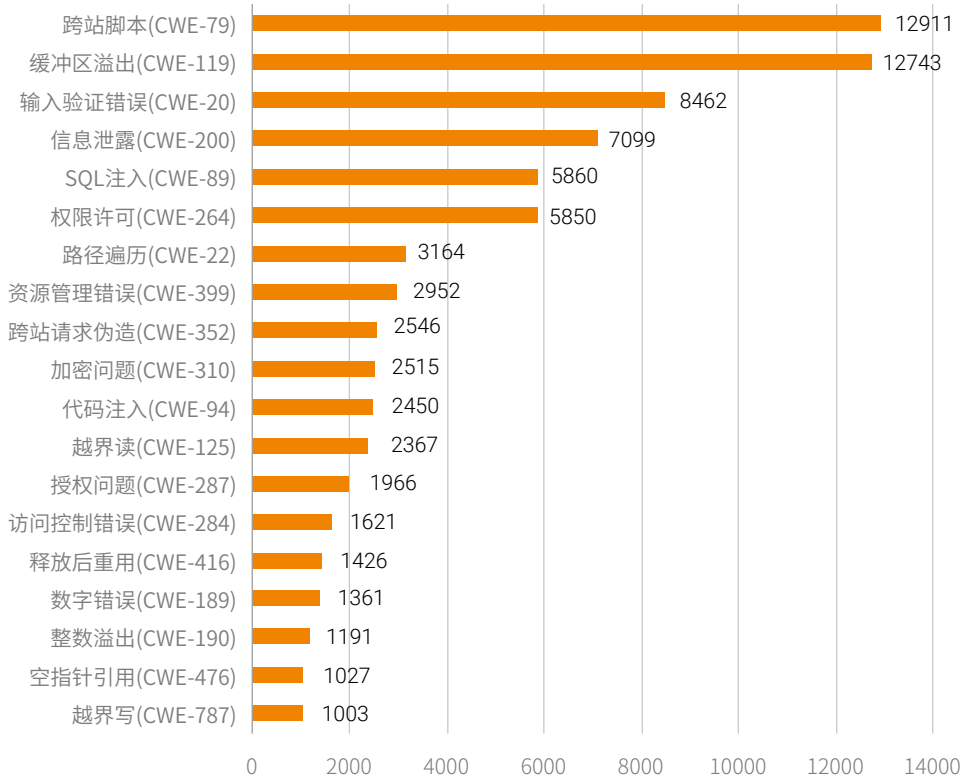



图 1.3 TOP20 CWE 漏洞类型

跨站脚本 (CWE-79) 类型的漏洞数量以 12911 条占据第一。其他传统的 Web 攻防技术也是屡见不鲜，SQL 注入 (CWE-89)、跨站请求伪造 (CWE-352)、代码注入 (CWE-94) 等常见于服务器及 Web 应用中，通过将恶意脚本嵌入到网页中，对网站数据造成危害。缓冲区溢出 (CWE-119)、越界读 (CWE-125)、释放后重用 (CWE-416)、空指针引用 (CWE-476) 以及越界写 (CWE-787) 代表内存错误类型的漏洞，此类型的漏洞在浏览器和 Office 软件中比较常见，同时也是 APT 攻击者的重要目标和武器。权限许可 (CWE-264) 和授权问题 (CWE-287) 以及访问控制错误 (CWE-284) 代表权限类型的漏洞，主要集中在服务器操作系统、数据库类的应用中。信息泄露 (CWE-200)、资源管理错误 (CWE-399) 等类型的漏洞能够导致敏感信息暴露，比如系统配置信息，数据库信息等，为攻击者进一步的攻击行为提供帮助。

## 1.2 通用软件产品的漏洞数量排名

根据 NVD 漏洞库统计了前 10 漏洞数量涉及的供应商，如图 1.4 所示，主要涵盖 Microsoft、Oracle、Google、IBM、Apple、Cisco、Debian、Adobe、Redhat、Canonical。其中 Microsoft 的漏洞累计 6996 个，在厂商中排名第一。

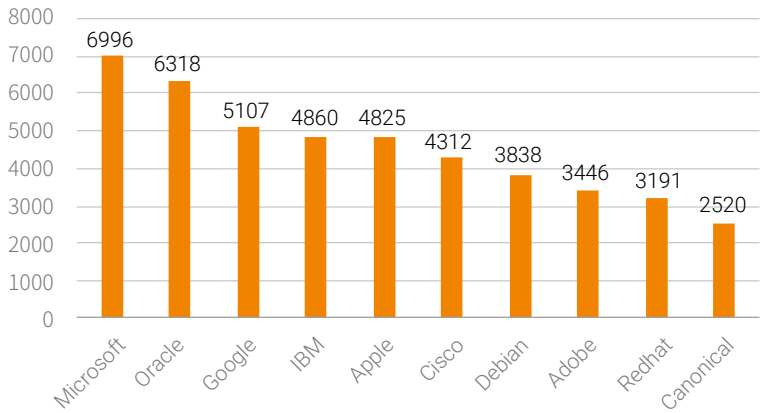



图 1.4 TOP10 漏洞数量供应商

Microsoft 公司众多操作系统、Google 公司的 Chrome 浏览器、Oracle 公司的 Java 运行时环境、Apple 公司的 iPhone、Adobe 公司的 Acrobat Reader 和 Flash，这些产品的用户基数大，实现功能复杂，导致被大量安全研究员所关注，漏洞数量相对较多。

### 1.2.1 操作系统漏洞排名

根据 NVD 数据库对 Product 字段的统计，操作系统的 TOP10 漏洞数量排名如图 1.5 所示[1]。主流的 Linux 发行版包含 Debian 和 Redhat，其中 Debian Linux 的系统稳定且占用内存小，软件包集成度良好，深受用户喜欢。Debian 其及社区能在软件发布中快速地修复安全问题，安全研究的投入也比较多，在过去的 20 年里累计发现了 3705 条漏洞。

1 发行版 Linux 的漏洞中不包含 linux kernel 的漏洞

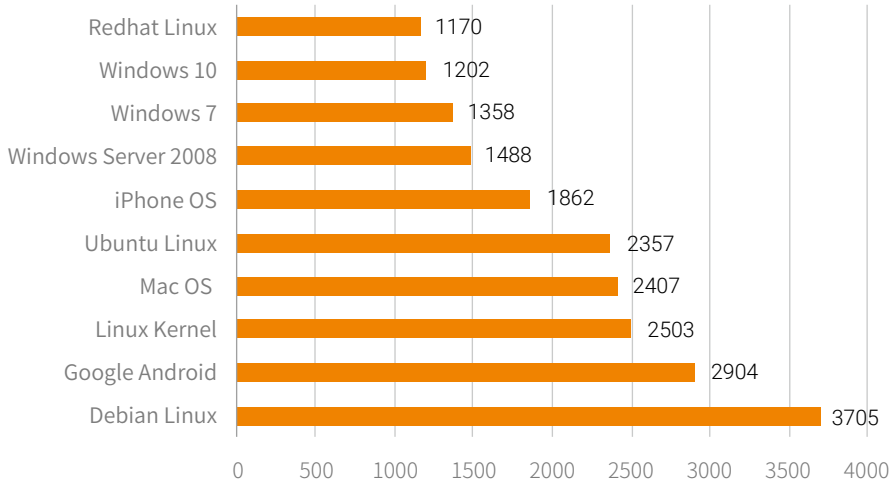



图 1.5 TOP10 操作系统漏洞

Apple 的 Mac OS 系统以及 iOS 系统漏洞排名第四及第六。Microsoft 的操作系统中，Windows Server 2008 的漏洞最多，排名第七，Windows 7 和 Windows 10 的漏洞数量紧随其后。

## 1.2.2 应用软件漏洞排名

应用软件的漏洞数量排名如图 1.6 所示[1]，Chrome 浏览器的漏洞排名第一， Firefox 排名第二、Internet Explorer 排名第四、Safari 则排名第五。Acrobat Reader 漏洞与 Adobe Flash 分别排名第三、第六。

1 Internet Explorer 的数量包含了 IE 和 Internet Explorer 字段的数量 ,Acrobat Reader 的数量包含了 Acrobat DC、Acrobat、Acrobat Reader、Reader 等字段的数量

## 历史漏洞回顾

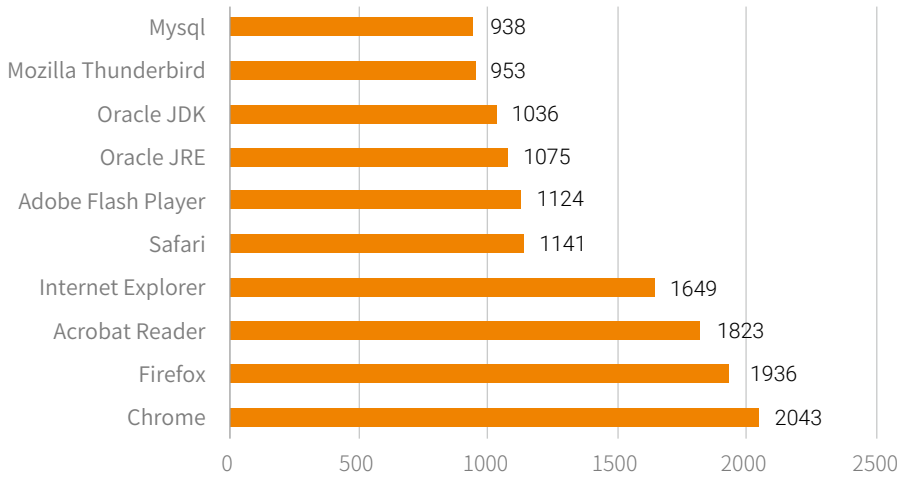



图 1.6 TOP10 应用软件漏洞

# 2

# 漏洞利用情况

## 2.1 典型漏洞攻击事件监测举例

漏洞利用是攻击的常用手段，通过对漏洞攻击事件的监测可以掌握攻击者的技术特点，行为习惯，进而可以对攻击者进行行为画像，为漏洞预警提供帮助，值得持续监测。本文重点关注 MS17-010 和 CVE-2019-0708 的攻击事件。

2017 年 4 月 Shadow Brokers 发布了针对 Windows 操作系统以及其他服务器系统软件的多个高危漏洞利用工具。同年 5 月 EternalBlue 工具被 WannaCry 勒索软件蠕虫利用，在全球范围大爆发，影响了包括中国在内的多个国家 [1]。EternalBlue 相关的漏洞主要有 CVE-2017-0144、CVE-2017-0145 以及 CVE-2017-0147，对应 Microsoft 的安全公告 MS17-010[2]。之后又陆续发生多起与 MS17-010 有关的勒索或挖矿木马攻击事件，WannaMine、PowerGhost、Satan 等众多恶意软件均利用了 MS17-010 进行传播。根据绿盟威胁情报中心监测到的 2019 年实际攻击事件显示，利用 CVE-2017-0144 的攻击事件共计 4919441 次，利用 CVE-2017-0145 的攻击事件共计 27276 次，利用 CVE-2017-0147 的攻击事件共计 1567618 次，按月分布的情况如图 2.1 所示。我们可以看到在 2019 年中，利用这些漏洞的网络攻击活动持续活跃在真实网络中。

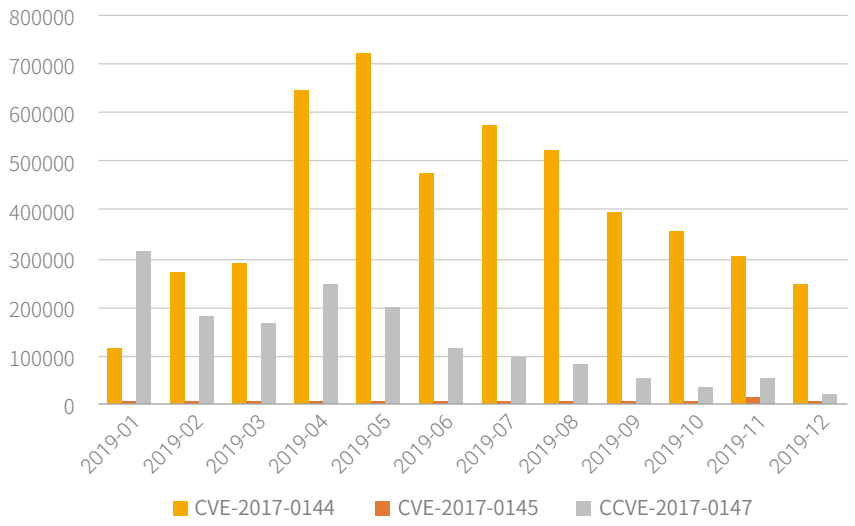



图 2.1 利用 ETERNALBLUE 漏洞的攻击事件

1 https://www.cert.org.cn/publish/main/9/2017/20170517075328471968938/20170517075328471968938_.html

2 https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

2019 年 5 月，Microsoft 在当月的安全更新中，对一个新的 RDP 漏洞 CVE-2019-0708[1] 发布了警告，该漏洞可以被用作蠕虫攻击，8 月又披露了两个类似的可用作蠕虫的漏洞 CVE-2019-1181/1182。随后的 9 月针对 CVE-2019-0708 的可利用攻击脚本已被公开 [2]。截止 2020 年 3 月，绿盟威胁情报中心监测到相关攻击事件 87211 次，如图 2.2 所示。在漏洞刚披露的 5 月份，漏洞的时效性强，并非所有用户都及时修复，漏洞利用价值高，高级攻击组织就会在网络中发起攻击，攻击事件出现了短暂的峰值。7 月份漏洞利用的代码被公开，更多黑产、脚本小子等攻击者开始使用，攻击事件再次呈现快速增长的趋势。随着攻击事件的持续发生，越来越多的用户开始更新补丁，修复漏洞，针对该漏洞的攻击事件逐渐下降。

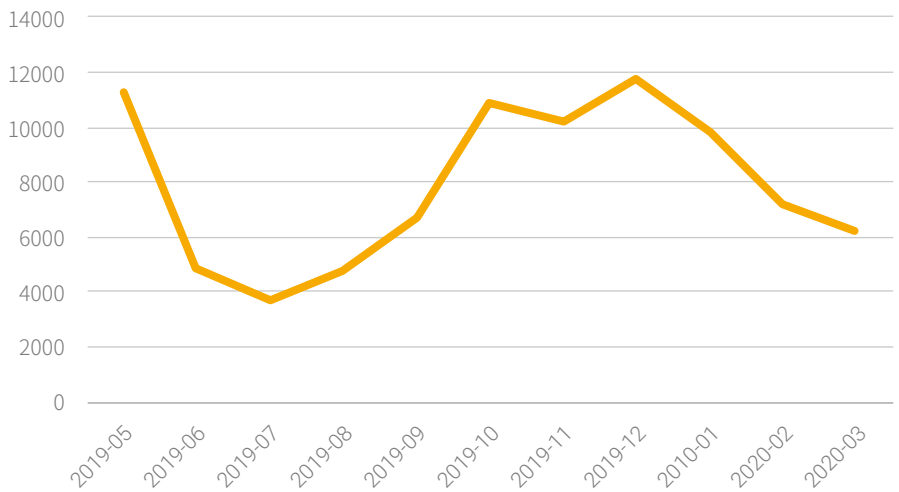



图 2.2 利用 CVE-2019-0708 漏洞的攻击事件

无论是开源软件还是闭源软件，一旦被攻击者抢先掌握漏洞的利用方式，并实现稳定的攻击工具，将对相关的软硬件设备造成重大的危害，对用户形成威胁。为了避免类似事件的发生，需要厂商、安全研究员携手共建安全生态。

1 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

2 https://www.exploit-db.com/exploits/47416

## 2.2 实际攻击中常用到 Nday 漏洞

攻击者关注稳定、高效的漏洞利用技术，对漏洞的选择上追求易用性、时效性以及是否能获取目标的控制权限的攻击能力。

根据绿盟威胁情报中心监测的安全事件，本文整理出了从 2019 年 1 月至 2020 年 3 月与漏洞利用相关的攻击事件，提取了漏洞利用比较高的 10 个漏洞信息，如表 2.1 所示。

表 2.1 漏洞利用较高的 CVE 信息

| CVE ID | 漏洞信息 |
| --- | --- |
| CVE-2002-2185 | ACK-Flood 拒绝服务攻击 |
| CVE-2017-0144 | Windows SMB 远程代码执行漏洞 (Shadow Brokers EternalBlue) |
| CVE-2017-12615 | Apache Tomcat 远程代码执行漏洞 |
| CVE-2003-0486 | phpBB viewtopic.php topic_id 远程 SQL 注入攻击 |
| CVE-2000-1209 | MSSQL 'sa' 用户执行登录失败 |
| CVE-2017-5638 | Struts2 远程命令执行漏洞 |
| CVE-2014-6271 | GNU Bash 环境变量远程命令执行漏洞 |
| CVE-2016-0800 | OpenSSl SSLv2 弱加密通信方式易受 DROWN 攻击 |
| CVE-2017-9793 | Apache Struts2 REST 插件拒绝服务漏洞 |
| CVE-2014-0094 | Apache Struts2 (CVE-2014-0094)(S2-020) 漏洞修补绕过 |

从日志中可以看到，攻击事件的发生不仅会用到近几年的漏洞，像 EternalBlue、Tomcat 远程代码执行这样好用的 Nday 漏洞也是黑客手中的利器，一些历史悠久的 SQL 注入、拒绝服务类型的漏洞，由于攻击门槛低，效果显著，攻击者依然在大量使用，使用到的漏洞按年份分布情况如图 2.3 所示。

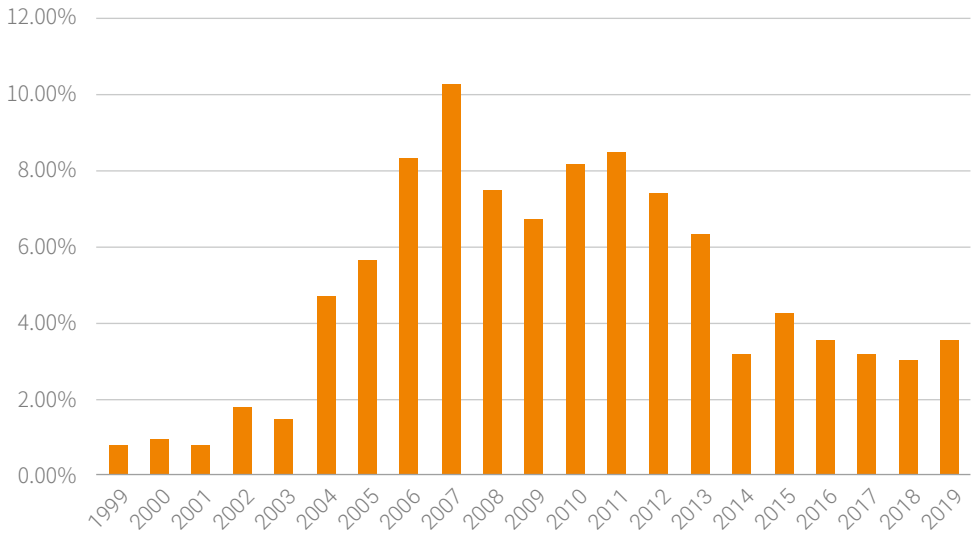



图 2.3 攻击事件使用到的漏洞按年分布

可以看到，即使是在 2019 年，10 年以上的高龄漏洞仍然占据了相当大的比例，说明互联网上依然存在着大量长期未更新的软件和系统。攻击事件中使用的漏洞和具体的操作系统环境相关，如物理隔离环境下的内网中，就可能存在没有及时更新补丁或版本的核心系统、数据库、系统和软件，攻击者一旦进入内网就可以利用这些成熟的漏洞利用代码发起有效的攻击。

总体来说随着时间的推移，老的漏洞会被不断的修补，与此同时又有新的漏洞不断产生，攻防之间的对抗将会一直持续。

# 3

# 漏洞发展趋势

## 3.1 浏览器漏洞种类复杂多样

浏览器作为用户访问互联网的媒介，为人们的工作、学习和生活带来了极大的便利。浏览器内部在运行时包含了各种复杂的过程，比如 DOM 树的解析、JavaScript 的动态执行、流媒体及协议的支持以及扩展与插件的实现。关于浏览器的漏洞研究一直是安全研究员关注的主要方向，同时浏览器与用户交互频繁的特点，也使其成为了攻击者的主要目标之一。主流浏览器的漏洞情况，如图 3.1 所示。

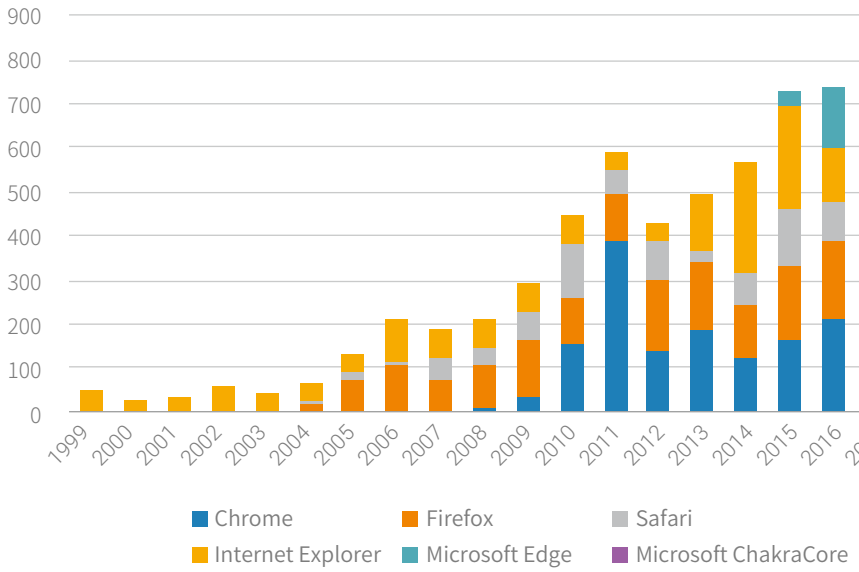



图 3.1 主流浏览器历年漏洞数量

主流的浏览器包括 Chrome、FireFox、Internet Explorer、Edge 以及 Safari，Web 端的漏洞主要类型有通用跨站脚本攻击 (UXSS) 和通用跨域漏洞；应用端的漏洞主要以内存破坏型漏洞为主，包含了缓冲区溢出、释放后重用、双重释放、越界读写等。

2009 年之前，Internet Explorer 作为 Windows 操作系统默认浏览器，占全球浏览器市场的份额最高，公布的漏洞数量也是最多的，此阶段的漏洞主要以 ActiveX 控件和基于栈的缓冲区溢出为主，通过简单暴力的超长字符串覆盖栈上保存的函数返回地址就可以控制程序的执行流程。为了提高内存数据的安全性，Microsoft 在 Windows 7 及后续系统中加入了数据执行保护、栈保护和堆栈地址随机化等多种新的安全机制，使得 2009 年后的一段时间内 Internet Explorer 漏洞呈现下降的趋势。

## 漏洞发展趋势

与此同时 Google 将 Chrome 浏览器的源代码开放，随着 Chrome 市场份额的增加，越来越多的安全研究员将视线转移过来，漏洞数量也随之增加。浏览器中对象众多且复杂，引起释放后重用 (UAF) 类型的漏洞大量出现，漏洞数量呈现上涨的趋势，Chrome 浏览器的漏洞数量也高居不下。

2013 年 Microsoft 启动 Mitigation Bypass Bounty 项目，对能绕过最新系统的防御措施的攻击技术，提供最高 10 万美元的奖励。此外，Google、Apple 等厂商也都推出漏洞悬赏计划，鼓励研究人员挖掘更多的产品漏洞，在这种利与名的双重驱动下，越界访问、释放后重用等新类型的漏洞一度呈现快速增长的趋势。

2014 年后 Microsoft 引入堆隔离和延迟释放等新的安全防护机制，同时在新版本操作系统中支持控制流保护，这些防护机制大大增加了漏洞利用难度和门槛。

2015 年 Microsoft 新发布了 Edge 浏览器，并作为 Windows 10 操作系统的默认浏览器，攻击者的目标也渐渐从 Internet Explorer 转向 Edge 浏览器，Edge 浏览器的漏洞数量逐渐上升，Internet Explorer 的数量逐渐下降。近年来，各大浏览器为了提高网页的加载和 JavaScript 脚本的运行速度，大量使用了即时编译 (Just-in-time) 系统，一时间 JIT 引擎成为攻击者主要的目标，大量因过度优化脚本代码导致数组长度，对象类型等校验错误的类型混淆和数组越界漏洞出现。

浏览器的漏洞总量近年来虽然略有下降，但将其作为攻击的入口在实际利用中深得攻击者的关注。根据绿盟威胁情报中心监测到的攻击事件，本文分析了应用软件漏洞利用分布，如图 3.2 所示，可以看到浏览器漏洞在网络攻击中达到了 48.44% 的比例，用户需要加强防护，尽快淘汰历史版本，及时打补丁，更新软件。

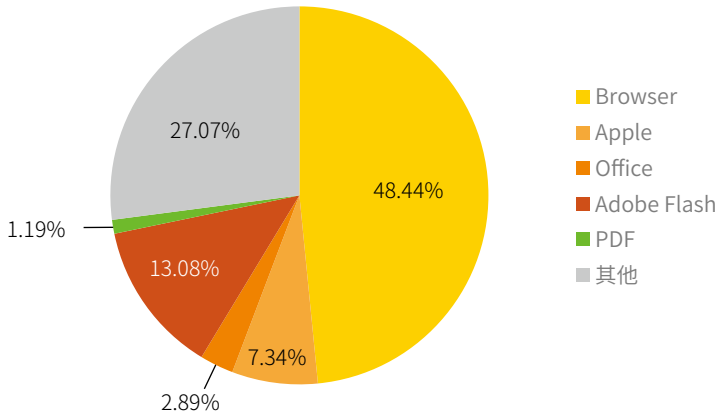



图 3.2 应用软件漏洞利用分布

## 3.2 文档类型漏洞利用情况解析

通过对 APT 攻击的研究发现，利用文件格式漏洞的鱼叉式钓鱼攻击已成为网络安全的主要威胁之一。PDF、doc(x)、xls(x)、ppt(x) 等文件格式具有跨平台、应用范围广、用户基数大的特点，受到了攻击者的持续关注，目标主机上的相应程序一旦存在安全漏洞就会被轻易攻破。本文统计了常见文档处理软件的漏洞分布，如图 3.3 所示。

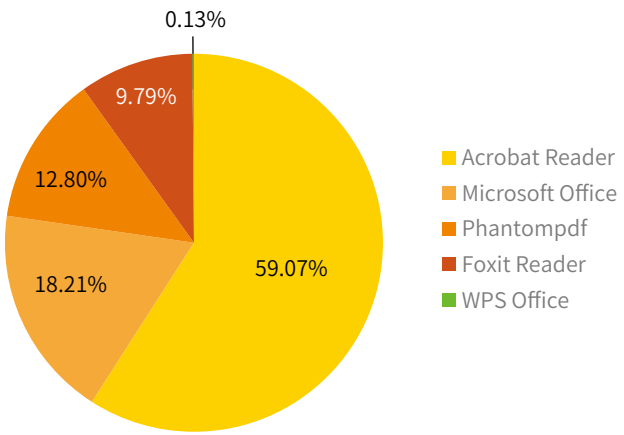



图 3.3 文档类型漏洞分布

## 漏洞发展趋势

Acrobat Reader 为载体的 PDF 漏洞数量共 1823 个，占据文档类型的 59.07%，PDF 文件格式复杂，支持 Javascript 脚本的执行，可以通过 Javascript 调用函数触发漏洞；支持嵌入图片 /XML 等外部文件，可以利用 PDF 中的关键字、XFA(XML Forms Architecture) 结构等嵌入远程文档以实现信息泄漏。

PDF 漏洞数量在常用文档处理软件中最多，但在实际攻击场景中利用却并不常见，最近的在实际场景中的漏洞利用要追溯到 2018 年 6 月的 CVE-2018-4990[1] Adobe Acrobat and Reader 堆内存越界访问释放漏洞，主要原因如下：

1. Adobe 公司在 PDF 阅读器软件上同时维护多条产品线。针对 PDF 格式文件阅读器的这一需求，Adobe 公司提供了 Adobe Acrobat 系列、Reader DC 系列以及已经停止维护的 Adobe Reader 系列产品。根据 Adobe 官方网站的介绍，每种产品的功能略有不同。通过对具体产品的分析调试可知，同一功能点在不同的产品中实现细节上会有些许差异。因此在其中一个产品上发现了漏洞，有一定概率不会在另一个产品上出现。如果将上图的接近 60% 的漏洞数量拆分的话，也会发现每种产品占比平均不到 20%，在正常范围内。更进一步说，即使在不同系列产品上发现了相同功能点的同一漏洞，为了在多款产品上可以成功触发利用，就需要进行适配。不但增加了攻击者的攻击成本，还会使最终的恶意文件体积臃肿，增加了被用户和防御工具发现的机会。另一方面用户使用版本的多样性也降低了攻击成功的几率。
2. Adobe 公司 PDF 阅读器自身防护的提高。2017 年 Adobe 公司在 Adobe Reader 10 中正式引入了沙箱机制。通过引入该机制，可以有效地阻止恶意代码的执行，并阻止对用户系统的提权行为，增加了攻击难度。
3. PDF 漏洞利用方式套路化。针对 PDF 的漏洞利用目前主要的方式为在 PDF 文件中嵌入 Javascript 脚本，通过 Javascript 脚本实现沙箱绕过及后续攻击步骤。一方面攻击脚本呈现套路化，有较为固定的模式，另一方面用户通常使用的 PDF 文件不会嵌入 Javascript 脚本。最终导致对包含恶意 Javascript 脚本的 PDF 文件检测率较高。

虽然 PDF 的在野利用不多，但是由于其自身的应用广泛，功能丰富，同时可以嵌入 Javascript 脚本的便利性等特点，针对 Adobe 公司 PDF 阅读器的漏洞利用成为了每年国际国内比赛上的一个重要项目。

1 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4990

Office 相关的漏洞数量虽然比 PDF 格式的要少，但在实际攻击中备受黑客关注，大部分 APT 组织也会选择利用 Office 的高危漏洞进行攻击。从早些年的 ActiveX 漏洞 CVE-2012-0158 到近些年新出的 OLE2Link 对象逻辑漏洞 CVE-2017-0199、公式编辑器漏洞 CVE-2017-11882、EPS 脚本解析漏洞 CVE-2017-0262 等，每一个漏洞的杀伤力都十分巨大。

早期 Office 漏洞主要发生在模块解析处理的过程中，随着 Microsoft 不断完善安全措施，对软件持续更新，现在的 Office 漏洞已经转向了通过链接、嵌入对象加载其他有漏洞模块。从实际攻击的角度看，由于 Windows 操作系统下，Microsoft 的 Office 系列办公软件的使用量占有绝对的优势，相比 PDF 而言，攻击者在准备 Word、Excel、PowerPoint 等 Office 系列软件的漏洞利用文档时，只需考虑版本兼容，不需过多考虑产品兼容，一个稳定的漏洞利用文档基本可以实现一个产品的全覆盖。同时从对实际攻击事件的检测可以看到攻击者在 Office 漏洞利用中更加偏向成熟稳定的漏洞，以 CVE-2017-11882 公式编辑器漏洞为主 [1][2][3] 。

## 3.3 Flash 漏洞面临消亡

Adobe 公司在 2005 年收购 Flash，并大力推广应用使其一度是漏洞挖掘人员的研究焦点，根据图 3.4 的历史数据可以看到，2015 和 2016 年爆出的漏洞总数占据整体数量的 55.09%。在 Hacking Team 泄露 CVE-2015-5122 和 CVE-2015-5199 这两个 0day 漏洞之后，更是给漏洞利用带来了通用的模板 [4]，但之后随着 Adobe 引入了隔离堆、Vector 长度检测、CFG 保护等安全机制，Flash 漏洞利用的门槛被加大了很多。

1 http://blog.nsfocus.net/netwire-ncov-19-0318/

2 http://blog.nsfocus.net/fuyinglab-0330/

3 http://blog.nsfocus.net/smokeloader-0407/

4 https://github.com/rapid7/metasploit-framework/tree/master/external/source/flash_exploiter

漏洞发展趋势

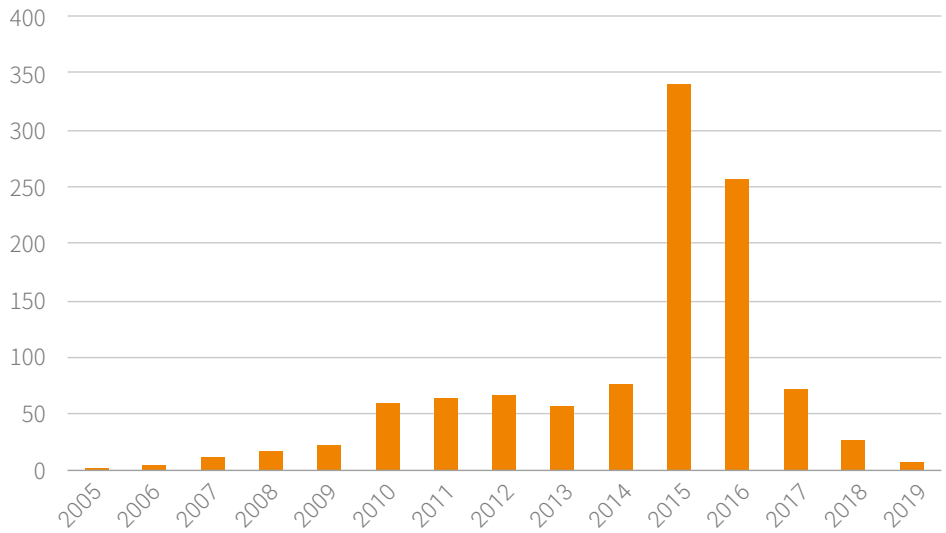



图 3.4 FLASH 历年漏洞数量

Flash 主要是通过 AVM2 虚拟处理器来解析执行 ActionScript3 脚本，并将其编译为 SWF 文件。但是 Flash 漏洞利用不能由单纯的 SWF 文件完成，需要在浏览器、Office、PDF 中以插件的形式来完成攻击。因此在实际攻击中 Flash 漏洞大都被嵌套在 Exploit Kit 工具包中，常见的有 Angler、Nuclear Pack 以及 Neutrino。这些工具包具有对环境进行侦查的特性，在各种环境下都可以稳定利用，更新速度快，并加入多种混淆手法来躲避安全软件的检测和拦截。攻击代码中通常将触发漏洞的 SWF 文件以 String 或者 ByteArray 的方式保存在变量中，然后通过 Loader 类的 loadBytes 方法来加载，或者通过内嵌二进制数据来存储加密后的关键字符串、混淆的函数名称或者函数类等。

2017 年 7 月，Adobe 宣布将在 2020 年底前逐步淘汰 Flash 插件，随后 Apple、Google、Microsoft 等厂商都对 Flash 采取了封杀机制，比如 Click-to-play 技术、沙盒技术。但是由于一些网站的适配支持、不及时更新的浏览器和系统等原因，互联网上的 Flash 应用并不会在短时间内完全消失，今后一段时间内，Flash 漏洞并不能彻底消亡，还需继续关注。

## 3.4 开源软件面临漏洞利用和软件供应链的双重攻击

开源软件具有开放、免费、功能灵活等特点，得到了越来越广泛的应用。通过公开源代码的行为，可以让更多人投入到软件的开发和维护中，安全研究人员可以通过白盒测试的方法对其进行漏洞挖

掘。但是开源软件的安全问题仍然普遍存在。本文统计了常见开源软件的漏洞数量，除 Linux Kernel、Chrome、Firefox 之外的排名如图 3.5 所示。

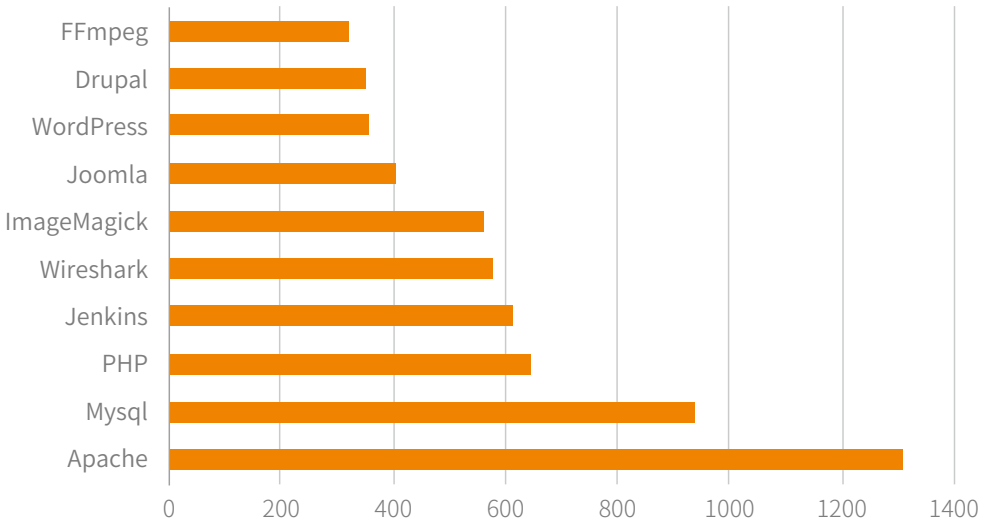



图 3.5 常见开源软件的漏洞数量

Web 框架及中间件也频频出现高危漏洞，包括无需身份认证的远程代码执行漏洞，比如 Apache、Jenkins、Joomla、WordPress、Drupal 等，此类漏洞深受黑客团伙青睐，公开的利用代码在短时间内被集成到成熟的攻击框架或木马程序中，进一步降低了漏洞利用的门槛，而从漏洞公布到被攻击者大规模利用的时间窗口也在进一步缩短，给安全厂商防护能力带来了更大的挑战。

Mysql 数据库是目前使用最为广泛的数据库之一，存在各种拒绝服务、提权漏洞，攻击者借助漏洞对数据库配置文件进行修改，获取数据库的 ROOT 权限，进而窃取数据以达到勒索或其他目的。

通常情况下，软件功能的复杂度和出现安全问题的概率是正相关的，比如网络协议分析利器 Wireshark、图片文件处理工具 ImageMagick、多媒体框架 FFmpeg 等，拥有复杂的处理逻辑，并且广泛使用，更容易成为研究员或者黑客的目标。

随着软件开源模式的兴起，除漏洞利用之外，针对软件供应链的攻击成为面向软件开发人员和供应商的一种新兴威胁。软件供应链主要包含开发、交付、使用三个阶段，攻击者一旦对软件供应链中的任意阶段进行攻击，都会引起软件供应链的连锁反应。2019 年 8 月，题为《杭州警方通报打击涉网违法

犯罪暨“净网 2019”专项行动战果》的文章披露了 phpStudy 存在“后门”。攻击者入侵 phpStudy 官网后，通过在 php_xmlrpc.dll 文件中插入后门代码，重新打包后替换了官网中的原版软件包，加上第三方下载站点也会受到污染，从而导致存在有后门的 phpStudy 广泛地传播开来。针对软件供应链的攻击相当于给攻击者的恶意代码披上了“合法”的外衣，在传播速度上更快，影响范围更广，危害更大，同时也更隐蔽。软件开发商应该制定软件供应链标准、规范，遵循安全的开发流程，定期组织软件供应链攻防演练、竞赛，定期对自身网站、软件等进行检测与加固以减少受到此类攻击的风险。

## 3.5 Android 和 iOS 漏洞加剧移动安全的威胁

智能手机及其终端应用程序与我们的生活越来越紧密，囊括了通讯、支付、社交、出行等各种用途。智能手机终端主要有 Symbian、Android 以及 iOS 三类操作系统。

诺基亚的 Symbian 系统曾一度风靡，现有漏洞只有 2 个，CVE-2006-4464 和 CVE-2009-2538。主要是由于在当时，系统的开放性还很低，手机的性能、功能还不足以实现复杂的交互操作，致使手机上的应用很少，关注也不多。

Android 是由 Google 开发的基于 Linux 内核的开源系统，市场份额大，基于 Android 的恶意软件迅猛发展，系统漏洞的不断出现更是加剧了移动安全的威胁。根据 NVD 统计到的 Android 相关的漏洞有 2902 个，历年漏洞数量如图 3.6 所示。

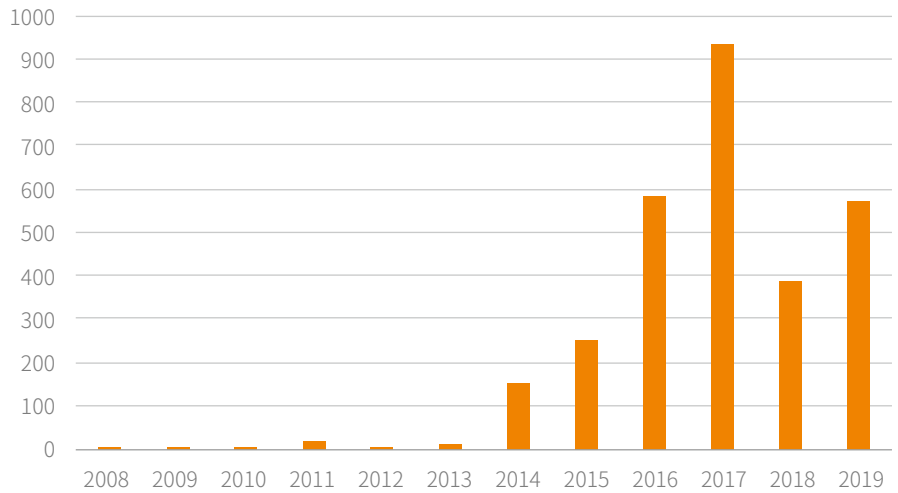



图 3.6 ANDROID 历年漏洞数量

## 漏洞发展趋势

可以看到自 2009 年起漏洞数量呈现增长的趋势。2015 年 Android 系统漏洞整体呈现爆发式增长。其中，Application Framework & Libraries 的漏洞总量达 130 个，同比上涨 1082%。2015 年 Android 的系统漏洞量涨幅迅速，主要原因是移动安全得到了越来越多的研究人员的关注。2018 年 8 月 Google 发布的 Android 9 中，为部分守护进程和内核引入了控制流完整性 CFI(Control Flow Integrity) 防护机制，能够直接对抗常用 ROP/JOP/COOP 代码重用利用技巧。新的保护机制的引入和 Google 对 Android 系统安全逐渐重视使得 2017 年后漏洞数量显著减少。

Linux 内核层的漏洞是影响范围最广的漏洞之一，能导致系统高级权限的泄露，恶意程序利用这些漏洞来提升自己权限从而肆意窃取数据。例如，CVE-2016-5195 脏牛 (Dirty COW) 是 Linux 内核的内存子系统在处理写时拷贝 (Copy-on-Write) 时存在条件竞争漏洞，导致可以破坏私有只读内存映射。一个低权限的本地用户能够利用此漏洞获取其他只读内存映射的写权限，有可能进一步导致权限提权。系统架构层作为 Android 系统的主体，它的漏洞会给使用框架层接口的所有应用带来安全威胁。例如，CVE-2017-13288、CVE-2017-13315 共同点在于框架中 Parcelable 对象的序列化和反序列化不一致，攻击者借此绕过安全软件对手机系统的保护，进一步攻击系统来获取更高的权限。第三方核心类库如 libc、SQLite、WebKit、SSL 等，在继承这些开源项目的同时也不可避免地继承了它们的漏洞。2019 年 10 月披露的 WhatsApp 远程 RCE 漏洞（CVE-2019-11932）正是因为引入的用于处理 GIF 图片的开源库 Android-gif-Drawable 存在 Double-Free 漏洞导致。该 GIF 开源库被大量安卓 APP 使用，全球范围内 43619 个使用该 GIF 开源库开发的安卓 APP 可能受此漏洞影响 [1]。

iOS 是由 Apple 为其手机、平板、Watch 等智能设备量身打造的操作系统，自从 2007 年推出第一代 iOS 智能手机以来，在移动市场的规模快速增长。该系统由于硬件与软件高度集成，一向以安全著称。攻击者想要获取操作系统的最高权限，就必须对设备进行越狱，而越狱需要依靠安全漏洞。iOS 系统相关的漏洞共 1862 个，历年漏洞数量如图 3.7 所示。

1 https://www.freebuf.com/news/218375.html

漏洞发展趋势

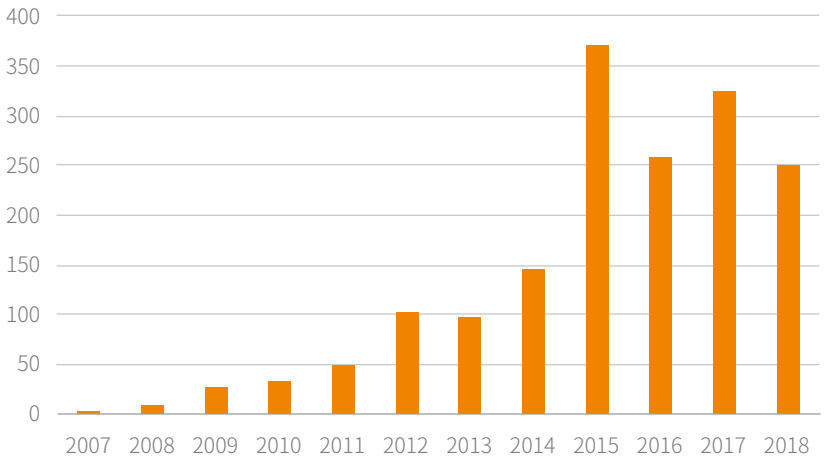



图 3.7 IOS 系统历年漏洞数量

2015 年 iOS 系统漏洞呈现爆发式增长，全年漏洞总量达 369 个，同比上涨 156.25%，例如，用于 iOS 9 越狱的 CVE-2015-6974 漏洞，CVE-2015-7037 Photos 沙盒逃逸漏洞，CVE-2015-7084 IORegistryIterator 内核漏洞等。增长的主要原因是关注 iOS 安全的研究人员变多，很多以前被忽略的系统攻击被发现并从中找到了漏洞提交给 Apple 修复。近 2 年来 Apple 应用的漏洞利用有个大幅度的提升。2019 年 8 月 Google 安全团队公布了 5 个漏洞利用链及相关联的 14 个安全漏洞 [1]，涉及从 iOS 10 到最新版本 iOS 12 的所有版本，这无疑为其他攻击者提供了一个很好的着手点，对 iOS 系统的安全性提出了巨大的挑战。

## 3.6 安全堪忧的 IoT 设备

物联网技术的成熟加速了智能家居的发展，接入网络的 IoT 设备数量和总类越来越多，从摄像头、路由器到电视机、空气净化器、扫地机器人、空调、热水器等都接入了网络。据市场研究公司 Gartner 称，2016 年全球物联网设备数量为 64 亿，2020 年将达到 204 亿 [2]，增长 218.75%。但是设备制造商并不

1 https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html

2 https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

太关心设备的安全性，防御措施少，很最容易被攻击者利用。表 3.1 给出了 2019 年物联网漏洞利用数量前 10 的漏洞信息。

表 3.1 TOP10 物联网漏洞利用数量

| CVE ID | 漏洞信息 |
|---|---|
| CVE-2015-2051 | D-Link Devices - HNAP SOAPAction-Header Command Execution |
| CVE-2017-17215 | Huawei Router HG532 - Arbitrary Command Execution |
| CVE-2016-10372 | Eir D1000 Wireless Router - WAN Side Remote Command Injection (CVE-2016-10372) |
| | AVTECH IP Camera / NVR / DVR Devices - Multiple Vulnerabilities |
| | MVPower DVR TV-7104HE 1.8.4 115215B9 - Shell Command Execution (Metasploit) |
| CVE-2014-8361 | Realtek SDK - Miniigd UPnP SOAP Command Execution (Metasploit) |
| | Shenzhen TVT Digital Technology Co. Ltd & OEM {DVR/NVR/IPC} API RCE |
| | Linksys Router |
| | Netgear DGN1000 1.1.00.48 - 'Setup.cgi' Remote Code Execution (Metasploit) |
| CVE-2017-8225 | Wireless IP Camera (P2P) WIFICAM - Remote Code Execution |

其中 CVE-2015-2051、CVE-2017-17215、CVE-2014-8361 这三个漏洞都与 UPnP 协议有关。UPnP 是由通用即插即用论坛制定的一套基于 TCP/IP 的网络协议，它使用 SSDP 协议来发现其他可用的设备和服务，使用 SOAP 协议实现对设备的控制。根据绿盟科技 2019 年物联网安全年报 [1]，SOAP 服务可访问的设备占 UPnP 设备总量的 46.9%，这些设备中，61% 的设备存在中危及以上的漏洞，攻击者可以通过漏洞获取对这些设备的完全控制权，或利用漏洞发动攻击使设备崩溃。

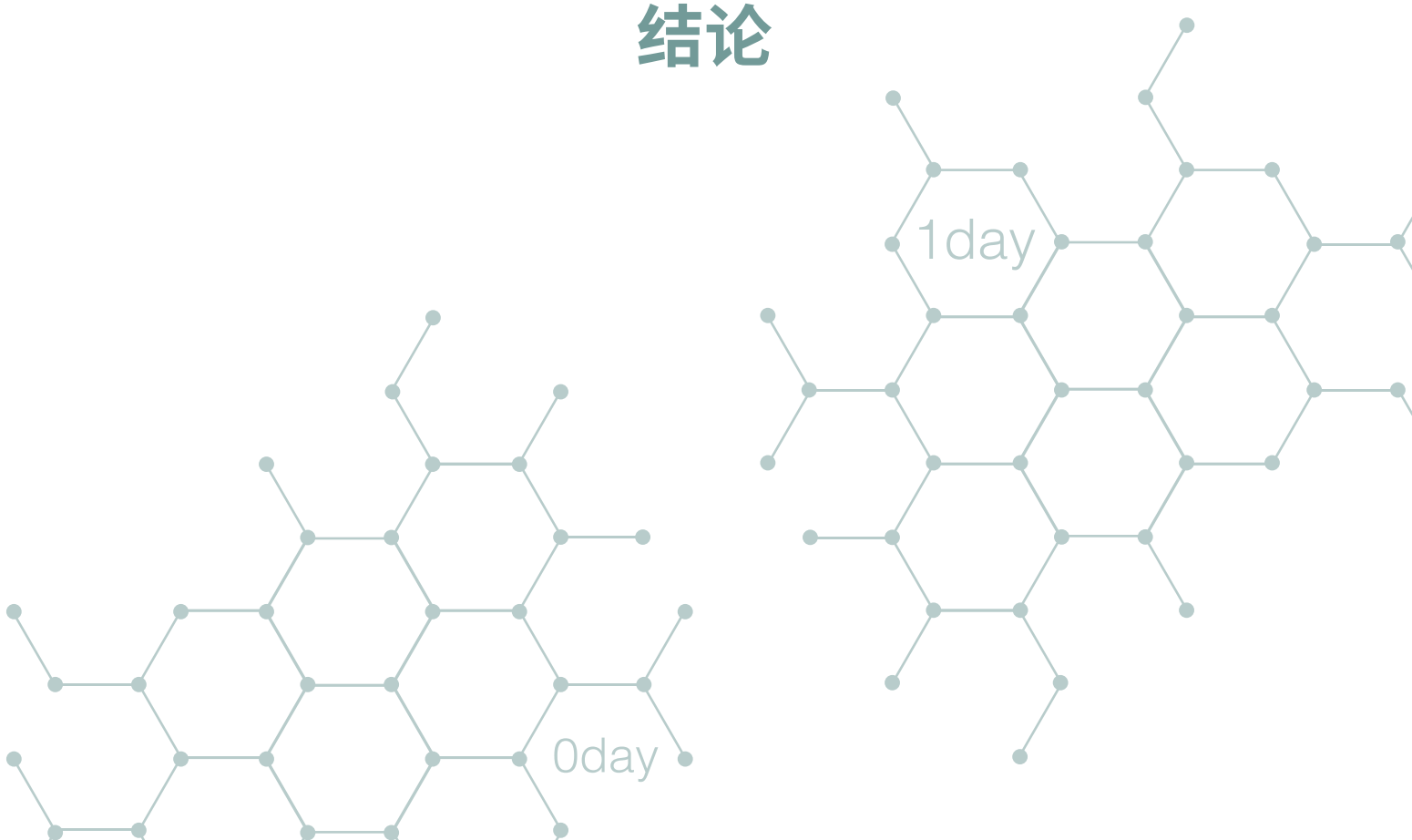
已经监测的漏洞利用所对应目标设备以路由器和视频监控设备为主。路由器作为智能家居的中心，连接着各种智能设备，是各种设备联网的基础，很容易成为黑客攻击其他设备的跳板。视频监控设备被攻破则可以用于监视其拥有者，让隐私暴露无遗，甚至会被敲诈勒索。这些安全问题主要来源于两点，一是由于大多数的固件在出厂时就存在弱口令、甚至无需口令校验的问题，这种不安全的固件配置大大提高了攻击者的攻击效率。二是固件所调用的第三方组件的漏洞甚至是操作系统内核漏洞不能够及时追踪修复。

面对物联网的威胁，设备制造商应当重视设备的安全，指定安全的开发流程，对设备进行全面的安全测试，对于默认密码的问题，应当在用户第一次使用的时候强制让用户修改密码，并检查用户密码的安全性，禁止设置弱密码。对使用周期较长的设备，定期提供可更新的固件，以确保设备的安全性。

1 https://www.nsfocus.com.cn/html/2019/92_1228/135.html

# 4

# 结论



## 结论

软件及其系统中的漏洞是导致信息安全问题的根源所在，如何减少安全漏洞已经成为了信息安全从业人员的热门话题。目前看来，这一愿景与漏洞数量逐年增长的趋势相悖。

安全是一个攻与防的过程，未知攻焉知防，只有在了解了各种攻击技术和手段后才能采取更加有效的防御策略，从而避免安全事件的发生。软件开发人员不仅需要具有熟练的编程技巧，还要拥有一定的攻防知识才能开发出相对安全的代码，并将安全属性融入到软件的开发过程中，从源头上尽量减少漏洞的产生。

安全研究人员需要加强系统漏洞及防护技术等方面的学习，不断深入地研究新的漏洞挖掘技术和利用技术，挑战各种漏洞的缓解措施，先攻击者一步掌握最新的攻击技术，才能与厂商携手进一步提高系统和应用的安全防护水平。

## 天机实验室

天机实验室专注于漏洞挖掘与利用技术研究。研究方向主要包括漏洞挖掘技术研究、漏洞分析技术研究、漏洞利用技术研究、安全防御机制及对抗技术研究等。研究目标涵盖主流操作系统、流行的应用系统及软件、重要的基础组件库以及新兴的技术方向。

## 绿盟威胁情报中心（NTI）

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技为落实智慧安全 2.0 战略，促进网络空间安全生态建设和威胁情报应用，增强客户攻防对抗能力而组建的专业性安全研究组织。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。


# THE EXPERT
## BEHIND GIANTS
## 巨人背后的安全专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供
具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com

绿盟科技官方微信