In the Boxing Ring
2026年4月

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2026年4月份的 In the **Boxing Ring**

本月，我们探讨开源安全。在层出不穷的网络威胁背景下，开源软件正重塑组织的防御方式。然而，开源软件往往众说纷纭：有人视其开放性为风险，也有人将其透明度视为优势。对于IT专业人士而言，关键问题不在于开源软件是否完美，而在于它能否提供比专有解决方案更强大、更快速、更具弹性的安全保障。事实表明，开源确实能够做到这一点，因此它已不再仅仅是一种选择，而是当今安全环境下的必然之选。第2至3页将对此进行深入讨论。

在第4页，我们重点介绍了本月“周二补丁”将为 Network Box 5 和8 以及我们的云服务发布的各项增强功能和修复内容。

其他新闻：Network Box香港参与了香港科技促进组（HKtag）主办的人工智能研讨会。此外，本月全球安全要闻报道了影响 Fortinet、谷歌 Chrome、思科、苹果 iOS 及TrueConf 的新发现漏洞。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 2026

本月摘要:

开源安全

在不断演化的网络安全环境中，开源软件（OSS）常常引发激烈争论。批评者以多起备受瞩目的漏洞为例，认为这表明开源软件存在固有弱点；而支持者则强调其透明性和协作精神。对于系统管理员、开发人员和安全工程师等技术从业者而言，　真正的问题在于：“与专有软件相比，开源软件能否提供更卓越的安全性？”现有证据有力地表明：答案是肯定的。凭借成千上万双眼睛对代码的严格审查、快速的补丁发布周期以及卓越的鲁棒性记录，开源软件的优势远远超过其不足。

透明度推动主动防御

开源软件的显著特征在于其源代码的公开可用性，这使得全球范围内的代码审查成为可能，而专有软件根本无法做到这一点。林纳斯定律——“只要有足够多的开发者围观，任何漏洞都算不上什么大问题”——在实践中得到了充分验证。像 Linux 内核、Apache HTTP 服务器和 OpenSSL 这样的项目，得益于来自世界各地专家的贡献，能够及时发现并修复那些单个厂商团队可能遗漏的缺陷。

以 Linux 内核为例：它既受到企业（如 Google、Red Hat 和 Intel）、学术界，也受到开源爱好者们的审计，其漏洞密度远低于 Windows 或 macOS 等同类系统。CVE 数据显示，针对严重漏洞的补丁通常在数天内发布，而且往往采取 preemptive 的方式提前修复，这得益于 GitHub 的 Dependabot 等工具，以及由社区主导的静态分析工具，例如 Coverity 扫描。这种“众人之眼”的效应在可 fork 的代码仓库中尤为明显：安全研究人员可以自行 fork 代码并加强安全性，而无需等待官方修复。

再对比闭源软件：二进制文件会掩盖漏洞，迫使用户完全依赖供应商的披露信息。例如， 当微软发布针对 EternalBlue（ CVE-2017-0144） 的补丁时，攻击者仅用数小时便对其进行了逆向工程，通过差异分析提取出可利用的漏洞利用代码。而开源软件则恰恰相反：漏洞信息是公开的，修复方案也同样公开，用户可以通过包管理器立即部署缓解措施。

快速修复
以及生态系统韧性

开源软件在响应速度上表现出色。OpenSSL 中的 Heartbleed 漏洞（CVE-2014-0160）暴露了一个影响数百万系统的缓冲区越界读取问题，但相关补丁却在 48 小时内发布到位，同时诸如 Nmap 脚本之类的工具也能立即检测出存在漏洞的服务器。社区通过邮件列表和缺陷跟踪系统（如 OSS-Security）进行漏洞分类和优先级排序，确保修复措施在整个广泛的用户生态中得到推广和应用。

然而，开源软件（OSS）模式也存在一些弊端。最显著的是，公开披露可能会加速攻击者的利用。以Log4j中的 Log4Shell漏洞（CVE-2021-44228）为例，在官方发布补丁之前，概念验证代码便已大量涌现，研究人员争相披露该漏洞。此外，项目分叉还可能导致“依赖地狱”——即一些无人维护的软件包长期处于脆弱状态。而且，并非所有开源软件都能获得足够的关注。小众库往往遭受冷落，而SolarWinds等供应链攻击事件则进一步凸显了在安全审查不到位时所存在的风险。

然而，这些相比专有软件固有的隐患仍显得微不足道。闭源补丁往往会引发漫长的逆向工程马拉松：Stuxnet 利用的零日漏洞就是在泄露后被彻底剖析的；而一些国家机构则会预先使用 Ghidra 等工具对 Windows 可执行文件进行逆向分析。开源软件的开放性从根本上杜绝了这种风险——攻击者无法从中获得不对称优势，而防守方却能直接查看相同的代码。审计结果也一再证明开源软件的优势：相比之下，闭源二进制文件往往充斥着未检查的缓冲区和薄弱的加密算法。

扩展信任
从平台到服务

各项指标进一步印证了这一观点。2023年Synopsys开源安全报告分析了1500多个项目：在高危漏洞方面，开源软件能在30天内修复85%的漏洞，而闭源软件的修复时间则不透明。GitHub的安全告警功能已主动修复了生态系统中90%的告警。以Ubuntu LTS分支为代表的Linux发行版，在补丁发布频率上已超越Windows；同时，SELinux 和AppArmor 等强制访问控制机制的引入，弥补了消费级Windows系统在这方面的缺失。

专有软件供应商往往会囤积漏洞以备不时之需（例如美国国家安全局的“永恒之蓝”漏洞泄露事件）， 从而延迟公开修复。而开源软件则要求通过负责任的渠道披露漏洞，这有助于建立社区层面的“免疫屏障”。经济激励机制也与此相契合：红帽公司每年投入数百万美元用于增强RHEL系统的安全性，并对上游项目Fedora提供资金支持。

拥抱开源

对于注重安全的工程师而言，开源软件并非完美，但它经过了实战检验。漏洞无处不在，然而开源软件的透明性、快速响应机制以及强大的社区力量，共同构筑起更为坚固的防护屏障。相比之下，闭源软件的“黑箱”特性往往会在补丁发布后仍被恶意利用；而开源软件则通过提前构建集体免疫来防患于未然。拥抱开源软件，但务必严谨审计：众目睽睽的优势终将胜出。

Network Box 5 和 8 新特性
2026年4月

2026年4月7日（星期二），Network Box 将发布本月的 周二补丁 “Patch Tuesday” 更新包，其中包含一系列功能增强与漏洞修复。各地区的 安全运营中心（SOC） 将在接下来的 14 天内分阶段推出这些新功能。

本月针对 Network Box 5 与 8 版本 的更新内容包括：

NBRS-5

- 增强的VPN监控：从NBRS-8回迁的改进功能，使VPN会话的日志记录和状态显示更加清晰。
- 灵活的平台选择：可根据平台选择BOX（NBRS-5、NBRS-8 等），以简化配置和部署。

NBRS-8

- 更智能的VPN可视化：日志记录与状态显示现提供更清晰的活跃会话信息，助力管理员更快排查问题。
- 灵活的平台选择：可根据平台选择BOX（NBRS-5、NBRS-8 等），以简化配置和部署。
- 更强大的威胁检测：部署“受感染局域网代理”签名集，以更有效地捕获已被入侵的流量。
- 增强的用户访问：改进的身份验证流程简化了用户门户GUI的登录体验。
- 细粒度Web控制：多层级URL分类实现更精准的过滤与策略执行。
- 高级 IPS 处理：中途会话接管和异步流支持提升了内联 IPS 的性能。
- 优化性能：多项细微改进，以提升整体速度、稳定性及可靠性。

在大多数情况下，以上更改不会影响正在运行的服务或要求设备重启。然而，在某些情况下（取决于配置），可能需要设备重启。如果需要，您的本地SOC将与您联系安排此事。

如果您需要关于上述任何内容的更多信息，请联系您的本地SOC。他们将安排部署和联络。

Network Box HIGHLIGHTS

Network Box 香港 HKtag AI 研讨会

Network Box香港参与了香港科技促进组（HKtag）主办的AI专题活动，主题为 ***生成式人工智能进校园—— 版权归属何方？数据由谁守护？***

随着人工智能教学工具迅速普及，教育工作者与校方管理者日益关注其带来的版权与数据安全风险。Network Box通过与教育工作者、IT协调员及学校管理者深入交流，进一步彰显其致力于提升香港教育界数字韧性，并支持建设安全、创新的智慧校园的承诺。

全球安全事件头条和漏洞情报

TechNadu

FortiGate边缘入侵导致深层网络沦陷及工作站被恶意控制

链接:
https://tinyurl.com/mtfuwzpa

Bleeping Computer

谷歌修复2026年遭攻击利用的第四个Chrome零日漏洞

链接:
https://tinyurl.com/3mbeutsc

Cyber Security News

思科IMC关键漏洞允许攻击者绕过身份验证

链接:
https://tinyurl.com/ywxa24ba

TechCrunch

苹果在iOS 26安全方面取得进展，但泄露的黑客工具仍使数百万人面临间谍软件攻击风险

链接:
https://tinyurl.com/mryzba8c

The Hacker News

TrueConf 零日漏洞在针对东南亚政府网络的攻击中被利用

链接:
https://tinyurl.com/3bcr4cj9

月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOC
cnnoc@network-box.cn

或者上门到:
深圳市福田区深南大道
竹子林求是大厦西座
920

+86 (755) 3336 1581

www.network-box.cn

翻译：Jason