

In the Boxing Ring

2024年4月



Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2024年4月份的 In the **Boxing Ring**

本月，我们要讨论的是 **CVE-2024-3094**，它让开放源代码社区和新闻电讯社热闹非凡。RedHat 已将该漏洞列为 10.0 级（最严重）。如果攻击成功，就可以在库中植入木马，从而攻击更大的目标。那么，问题到底是什么，它对开源社区有什么影响？我们将在第 2 页至第 3 页进行详细分析和讨论。

此外，Network Box 新加坡在“亚太商业客户服务卓越大奖 2024”荣获最具价值网络安全解决方案公司大奖。此外，Network Box 香港协助警方对其 Scameter+ App 进行红队检测。在本月的科技聚焦中，我们特别介绍 Network Box 的移动 SIEM+ 应用。此应用适用于苹果 iOS 及 Android 移动装置，让用户安全地管理 Network Box 的管理服务。



Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 2024

本月摘要:

第2-3页

CVE-2024-3094: 在库中植入木马以攻击更大的目标

早些时候，开源社区和新闻机构都在热议 CVE-2024-3094 的发布。该漏洞被 RedHat 评为 10.0 级，如果攻击成功，恶意行为者就可以登录任何设置为远程访问的系统，并运行木马代码。在我们的专题文章中，我们将更详细地讨论这个问题及其影响。

第4页

Network Box 亮点:

- **Network Box 新加坡:**
最具价值网络安全解决方案公司 - 2024 年亚太地区企业客户服务卓越奖。
- **Network Box 香港:** HKPF Scameter+ App 专访
- **Network Box 技术聚焦:**
Network Box 移动 SIEM+ App



CVE-2024-3094: 在库中植入木马以攻击更大的目标

在 3 月 29 日发布 CVE-2024-3094 之后，开源社区和新闻电讯在过去几天里一直很热闹。

RedHat 将其归类为 10.0（最严重），该安全公告概述了问题所在：

从 5.6.0 版开始，在 xz 的上游压缩包中发现了恶意代码。

通过一系列复杂的混淆处理，liblzma 编译过程从源代码中存在的伪装的测试文件中提取了一个预编译对象文件，然后用来修改 liblzma 代码中的特定函数。这样就产生了一个经过修改的 liblzma 库，任何与该库链接的软件都可以使用它，拦截并修改与该库交互的数据。

那么问题到底出在哪里，对开源社区又有什么影响呢？

xz 是什么？

开源实用程序“xz”（及其提供的库）用于使 LZMA 压缩在免费操作系统上易于使用。这是通过提供与最流行的现有压缩算法类似的工具和库来实现的。Lempel-Ziv-Markov 链算法 (LZMA) 自 20 世纪 90 年代以来就已出现，多年来已在许多不同的产品中使用。

为什么要木马该库？

虽然目标可能是所提供的 "xz" 命令行实用程序，但在本例中似乎并非如此。对问题的分析还处于初期阶段，但 liblzma 似乎不是主要目标。相反，目标可能是一个非常流行的 LZMA 库用户 "OpenSSH"。

攻击者为 xz 项目贡献了代码，但他们并没有在代码中提供木马后门（其他项目维护者相对容易发现），而是将木马代码混淆并隐藏在多个测试用例中。这些测试用例通常在库的生产构建过程中运行，而这一次，测试用例将后门动态地部署到了构建好的库中。这种方法相当隐蔽，而且非常有效。但更复杂、更不可靠。



其目的似乎是在用于远程安全 shell（通常是管理）系统访问的 SSHD 服务中插入木马代码。代码拦截了 SSHD 用于验证远程用户身份的机制，似乎是硬编码，接受特定的公钥（可能是攻击者的公钥）。但是，如前所述，现在还时尚早，我们仍在努力研究其影响（以及该特定贡献者向 xz 项目提交的约 700 次代码）。

有什么影响？

最坏的情况似乎是，如果攻击成功，攻击者就可以登录任何设置为远程访问的系统，并运行木马代码。

但要做到这一点，还需要做很多事情：

1. 需要以正确的方式构建代码，才能将木马程序内置到程序库中。
2. 这一点需要不引起注意。
3. 在构建 OpenSSH 时需要选取并包含该库。
4. 这一点需要不引起注意。
5. 需要将 OpenSSH 服务器部署/更新到易受攻击的版本。
6. OpenSSH 服务器需要设置为接受使用公钥进行身份验证（大多数情况下都是如此）。
7. OpenSSH 服务器需要能访问互联网。

应特别强调第 7 点（最后一道防线）--远程管理访问绝不应直接向互联网开放。我们过去曾撰文介绍过这一最佳实践，它仍然是 Network Box 安全响应团队所见过的网络中的头号漏洞。

在开源和闭源开发项目中，此类供应链攻击并不罕见。尽管如此，与往常一样，反对者还是抓住了这个机会，试图诋毁开源软件。然而，在这种情况下，开源的效果是可以预期的，而且很可能比闭源要好得多。首先，问题很早就发现了。一位用户注意到一些时间差异，由于代码是开源的，他查找并发现了问题。项目社区收到了警报，案件升级，几天之内所有主要发行版都发布了补丁、缓解措施或无影响声明。幸运的是，它很快就被发现了，没有一个主要发行版受到影响（至少对于他们发布的代码来说）。

Network Box 5 平台和即将推出的 NBR5-8 都不受此影响。如果没有开源—所有的眼睛都在盯着代码—事情可能会变得更糟。

Network Box HIGHLIGHTS



Network Box 香港 HKPF Scameter+ App 专访

Network Box 最近协助香港警务处在警方的 Scameter+ App 上执行红队检测，帮助用户避免网络和电话欺诈。Scameter+ App 可保护用户免受诈骗，而不会危及任何人的隐私。Scameter+ App 在设计上尊重每个用户的隐私。采访由香港无线电视进行。



Network Box 新加坡 新加坡商业奖 2024

Network Box 很高兴地宣布，公司在 2024 年亚太地区商业客户服务卓越奖评选中荣获 "最具价值网络安全解决方案公司" 大奖。



您知道吗.....

您可以使用 Network Box 移动 SIEM+ 应用程序访问工单系统并查看网络活动？

Network Box 移动 SIEM+ 应用程序适用于手机和平板电脑、Apple iOS 和 Android 移动设备，旨在提供安全访问来管理 Network Box 托管服务。iOS 和 Android 平台上都提供了等效的功能。

该应用程序支持 Box Office / NBSIEM+ 用户帐户身份验证，并完全支持双因子身份验证（使用 RFC-6238 TOTP 标准）。

此外，它还与 Box Office 通知系统集成，支持 iOS 和 Google 通知系统。您可以使用 Box Office 按类型、时间范围、资产/BOX组等配置通知首选项。



更多详情，请参阅移动 SIEM+ 白皮书：

<https://mcdn.network-box.com/WhitePaper/NBWP-MobileSIEM.pdf>

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 CNNOCC
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