In the Boxing Ring
APR 2024

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the April 2024 edition of In the **Boxing Ring**

This month, we are talking about **CVE-2024-3094**, which has the open source community and news wires buzzing. RedHat has classified the flaw as 10.0 (most critical). If successful, it would allow a trojan horse to be planted in a library to go after a bigger target. So what exactly is the problem, and what is its impact on the open source community? On pages 2 to 3, we break it down and discuss in greater detail.

In other news, Network Box Singapore won the **Best Value Cyber Security Solutions Company** award at the ***APAC Business Client Service Excellence Award 2024***. Additionally, Network Box Hong Kong assisted the Police Force in performing Red Teaming on the Police's **Scameter+ App**. And in this month's ***Technology Focus***, we are spotlighting the **Network Box Mobile SIEM+ App**. Available for both Apple iOS and Android-based mobile devices, the App provides secure access to administer Network Box managed services.

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

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse
https://www.linkedin.com/company/network-box-corporation-limited/
https://www.youtube.com/user/NetworkBox

In this month's issue:

CVE-2024-3094:
Planting a trojan horse in a library to go after a bigger target

The open source community and news wires have been buzzing for the past few days after the 29th March release of CVE-2024-3094.

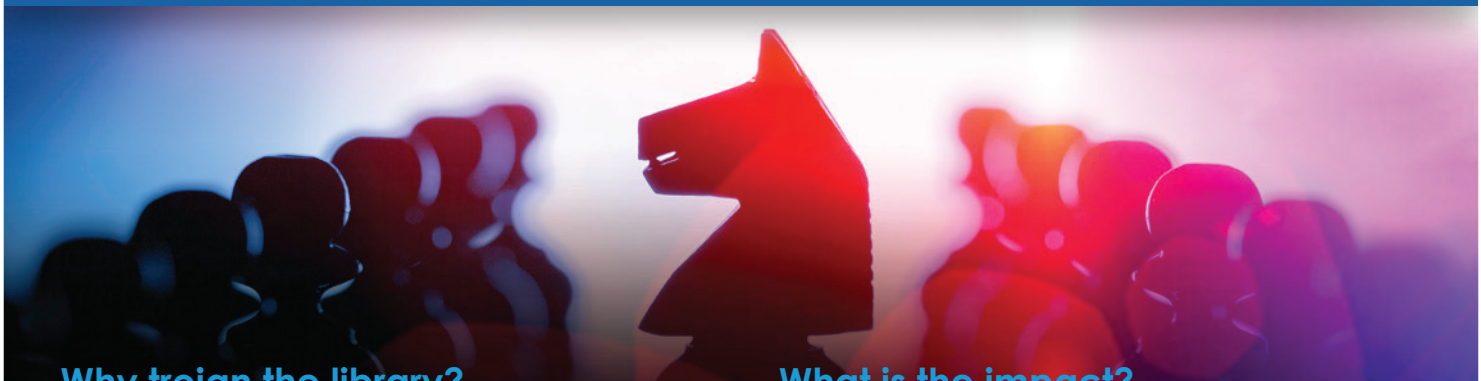
Classified by **RedHat** as 10.0 (most critical), the security advisory outlines the problem:

> *Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library.*

So what exactly is the problem, and what is the impact on the open source community? Let's break it down.

What is xz?

The open source utility 'xz' (and its provided library) are an attempt to make LZMA compression easy to use on free operating systems. This is achieved by providing tools and libraries similar to the equivalents of the most popular existing compression algorithms. The Lempel–Ziv–Markov chain algorithm (LZMA) has been around since the 1990s and has been used in many different products over the years.



Why trojan the library?

While the target could have been the provided 'xz' command-line utility, that does not seem to have been the case in this instance. Analysis of the problem is in its early days, but it seems that liblzma was not the main target. Instead, the target was a very popular user of the LZMA library called 'OpenSSH.'

The attackers contributed code to the xz project, but rather than just providing trojan horseback doors in their updates (which would have been relatively easy to spot by other project maintainers), they instead provided the trojan code obfuscated and hidden in several test cases. These test cases are typically run during the production building of the library, and this time, the test cases deploy the back door dynamically into the built library. Rather sneaky and very effective. But more complex and less reliable.

The goal appears to have been to insert the trojan code into the SSHD service used for remote secure shell (usually administrative) system access. The code intercepts the mechanism SSHD uses to authenticate remote users and appears to be hard-coded, accepting a particular public key (presumably that of the attacker). But, as said earlier, it is early days, and work is still being done on the impact of this (as well as the approximately 700 code commits this particular contributor has made to the xz project).

What is the impact?

The worst-case scenario, it seems, is that if successful, the attacker would have login access to any system set up for remote access and run the trojaned code.

But a lot of things need to happen for that to occur:

1. The code build needs to be done in the right way for the trojan to be built into the library.
2. That needs to go unnoticed.
3. The library needs to be picked up and included by an OpenSSH build.
4. That needs to go unnoticed.
5. The OpenSSH server needs to be deployed/updated to the vulnerable version.
6. The OpenSSH server needs to be configured to accept authentication using public keys (most are).
7. The OpenSSH server needs to be accessible to the Internet.

Point **#7** in particular (the last line of defense) should be stressed - remote administrative access should never be directly open to the Internet. We have written about this best practice in the past, and it continues to be the #1 vulnerability in networks that Network Box Security Response has seen.

Such supply chain attacks are not unusual in open and closed source development projects. Still, as usual, the naysayers jumped at the opportunity to try to denigrate the open source software approach. However, in this case, the open source approach worked out as well as can be expected and most likely significantly better than a closed source equivalent. Firstly, the problem was found very early. A user noticed some timing discrepancies, and as the code was open source, he looked for it and found the problem. The project community was alerted, the case escalated, and within a couple of days all the major distributions had released patches, mitigations, or statements of non impact. Thankfully, it was caught quickly enough that none of the major distributions were affected (at least for their released code).

Neither the Network Box 5 platform nor the upcoming NBRS-8 is affected by this. Without open source, all those eyes looking at the code, things could have been so much worse.

Network Box HIGHLIGHTS

Network Box Hong Kong
HKPF Scameter+ App Interview

Network Box recently assisted the Hong Kong Police Force in performing Red Teaming on the Police's **Scameter+ App**, which helps users avoid both Web and Phone fraud. The key takeaway is that the Scameter+ App protects users from being scammed without risking anyone's privacy. The Scameter+ App respects each user's privacy by design. The interview was conducted by TVB HK.

Network Box Singapore
Singapore Business Awards 2024

Network Box is pleased to announce that the company won the ***Best Value Cyber Security Solutions Company*** award at the **APAC Business Client Service Excellence Award 2024.**

Network Box Technology Focus

Did you know...
You can access the Box Office ticketing system and view your network activities using the Network Box Mobile SIEM+ app?

Available for phones and tablets, for both Apple iOS and Android-based mobile devices, the Network Box Mobile SIEM+ App is designed to provide secure access to administer Network Box managed services. Equivalent functionality is provided on both the iOS and Android platforms.

The App supports Box Office / NBSIEM+ user account authentication and fully supports dual-factor authentication (using the RFC-6238 TOTP standard).

In addition, it integrates into the Box Office notification system, supporting iOS and Google notification systems. You can use Box Office to configure the notification preferences by type, time range, asset/box group, and more.

For more details, please refer to the Mobile SIEM+ whitepaper:

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

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong.

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com