CyMinded Security Report

Subject Matter: CVE-2024-3094

CVE-2024-3094 \ XZ Utils Backdoor:

A supply chain backdoor attack that was discovered in XZ Utils allowed the potential RCE via SSH authentication in Linux distributions.

XZ Utils is a library that handles file compression, based on the LZM algorithm, its Open

Source API is called Liblzma and is used by many softwares for compression purposes.

The vulnerability was discovered by Andres Freund after he noticed that ssh processes consumed high amounts of CPU – 10x more time.

The Cause: a GitHub account called "Jia Tan" who was a regular contributor of the xz\liblzma library contributed an obfuscated test file, but it wasn't just another test file.

How it started: in version control was a series of obfuscating make .xz files and binary files that were used to "test" the *liblzma*, this was the first backdoor, it was obfuscated to degrees the change of being found by strings, the first file calls a second file that created a .txt file which included a build process.

So far, the attacker's commits looked like regular library commits, but then he injected a new crc64 binary object, and while claiming he just made some changes to the algorithm, he changed existing functionalities of the crc functions and added a new one too, by injecting the above, a backdoor was installed into the liblzma, into the upstream repository and the xz tarballs.

In version 5.6.1 the attacker made a suspicious change, he removed the symbol names and obfuscated them, this is against coding transparency policy, where code should be clear to read,

This whole process allowed the attacker to corrupt and intercept SSH calls, by using the existing backdoor, he inserted an audit hook that acted as the middleman to the dynamic linker that collects data and functions paths for the SSHD program, specifically looking for RSA_public_dectypt function, so he could get the public key details and redirect it to malicious code, allowing him to intercept and manipulate SSH networking packets and potentially get the sensitive information of millions of users all around the globe.

CVSS Score: 10 – CRITICAL since the attacker compromised a widely used core library, Liblzma, with sophisticated backdoor that potentially could intercept SSH packets, exposing sensitive data at scale and enabling potential RCE.

Affected Products: XZ Utils versions 5.6.0 and 5.6.1 over Fedora, Debian, Kali Linux, OpenSUSE, Alpine, Arch and Gentoo, FreeBSD and Amazon Linux were not affected.

Potential Hacker Exploitation: as detailed above, the attacker exploited this vulnerability by inserting a backdoor into Liblzma, using it to manipulate the dynamic linker, intercept SSH traffic, steal sensitive data, and enable potential RCE.

Mitigation And Prevention: it was recommended to downgrade the uncompromised XZ Utils version, and hunt for any malicious or suspicious activity on systems where affected versions have been installed.