مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability Backdoor in XZ library

Tracking #:432315739

Date:01-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been discovered in the xz data compression library, commonly used in Linux distributions.

TECHNICAL DETAILS:

A critical security vulnerability (**CVSS score: 10**) has been discovered in the xz data compression library, commonly used in Linux distributions. This vulnerability allows for a malicious backdoor to be potentially installed, granting unauthorized remote access via SSH.

Critical Vulnerability Details:

- **CVE-2024-3094** (CVSS score: 10,Critical): Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0.

Affected Versions:

- xz versions 5.6.0 and 5.6.1
- Current reports indicate that the packages are only present in Fedora 41 and Fedora Rawhide within the Red Hat community ecosystem.
- No versions of Red Hat Enterprise Linux (RHEL) are affected.
- XZ Utils may be present in other Linux distributions such as Debian unstable (Sid), Alpine edge, Arch Linux, openSUSE Tumbleweed, and openSUSE MicroOS.

Fixed Versions:

- Fedora Users: Update to the patched version of xz as soon as possible. For Rawhide users, consider avoiding the system for now as it might be rolled back to a previous xz version.
- Other Linux Users: Check your distribution's update channels to see if xz 5.6.0 or 5.6.1 is installed and update accordingly.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to downgrade XZ Utils to an uncompromised version or install the patches and hunt for any malicious activity.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users