National Cyber Security Centre

2403290139-NCSC

**Department of the Environment, Climate & Communications**

# NCSC Alert

## Critical Vulnerability in XZ Utils (CVE-2024-3094)

**UPDATE**

Saturday 30th March, 2024

**STATUS:** TLP-CLEAR

*Recipients can spread this to the world, there is no limit on disclosure. Sources may use* TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

# Revision History

| Revision | Date | Author(s) | Description |
|---|---|---|---|
| 1.0 | 29th March 2024 | CSIRT-IE | Initial advisory |
| 1.1 | 30th March 2024 | CSIRT-IE | Updated impacted products |

## Description

**Published:** 2024-03-29T17:15:00
**Product:** XZ Utils Data Compression Library
**CVE ID:** CVE-2024-3094
**CVSS3.0 Score**[1]**:** 10.0

**Summary:** Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. The tarballs included extra .m4 files, which contained instructions for building with automake that did not exist in the repository. These instructions, through a series of complex obfuscations, extract a prebuilt object file from one of the test archives, which is then used to modify specific functions in the code while building the liblzma package. This issue results in liblzma being used by additional software, like sshd, to provide functionality that will be interpreted by the modified functions.

XZ is a general purpose data compression format present in nearly every Linux distribution, both community projects and commercial product distributions. Essentially, it helps compress (and then decompress) large file formats into smaller, more manageable sizes for sharing via file transfers. The xz-utils include the liblzma library used by various software including sshd which is one of the known techniques to abuse the backdoor.

More information related to this issue can be found at the links in the Recommendations section below.

## Products Affected

- XZ Utils versions 5.6.0 and 5.6.1
- Archlinux xz packages prior to version 5.6.1-2 (specifically 5.6.0-1 and 5.6.1-1)
- Fedora 41 and Fedora Rawhide
  - Out of an abundance of caution, Fedora Linux 40 users have been recommended to downgrade to a 5.4 build.
- Kali Linux (between March 26th and 29th)
- openSUSE Tumbleweed and openSUSE MicroOS (between March 7th and 28th)
- Debian testing, unstable, and experimental versions (from 5.5.1alpha-0.1 to 5.6.1-1)
- Redhat have advised that they have had reports and evidence of the injections successfully building in xz 5.6.x versions built for Debian unstable (Sid). Other distributions may also be affected. Users of other distributions should consult with their distributors for guidance.

## Impact

- **Common Weakness Enumeration (CWE)**[2]**:** Embedded Malicious Code
- **Present in CISA Known Exploited Vulnerability(KEV)**[3] **catalog:** NO

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://cwe.mitre.org/
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- **Used by Ransomware Operators:** Not Known

The malicious code may allow unauthorised access to affected systems.

## Recommendations

The NCSC strongly advises affected organisations to **immediately** stop using Fedora 41 or Fedora Rawhide, and to downgrade XZ Utils to an uncompromised version such as XZ Utils 5.4.6 Stable. If you have versions 5.6.0 or 5.6.1 installed, the NCSC advises that you review your system logs for suspicious activity. Additionally, for those running openSUSE distributions, SUSE has published a downgrade procedure at https://build.opensuse.org/request/show/1163302.

Additional recommendations for CVE-2024-3094 can be found in the respective link's below:

- https://www.openwall.com/lists/oss-security/2024/03/29/4 (Original Report)
- https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27
- https://access.redhat.com/security/cve/CVE-2024-3094
- https://bugzilla.redhat.com/show_bug.cgi?id=2272210
- https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users
- https://lists.debian.org/debian-security-announce/2024/msg00057.html
- https://www.tenable.com/blog/frequently-asked-questions-cve-2024-3094-supply-chain-backdoor-in-xz-utils

**DISCLAIMER:** This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
**Tel:** +353 (0)1 6782333
**Mail:** certreport@ncsc.gov.ie
**Web:** ncsc.gov.ie
**Twitter:** ncsc_gov_ie
**LinkedIn:** ncsc-ie