



# XZ has a heap-use-after-free bug in threaded .xz decoder

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-31115
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-04-03 17:15:30 UTC
<b>Updated</b>	2026-05-12 13:16:40 UTC

**Description** XZ Utils provide a general-purpose data-compression library plus command-line tools. In XZ Utils 5.3.3alpha to 5.8.0, the r

## Risk And Classification

**Primary CVSS:** v4.0 8.7 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000410000 probability, percentile 0.125130000 (date 2026-05-12)

**Problem Types:** CWE-366 | CWE-416 | CWE-476 | CWE-826 | CWE-366 CWE-366: Race Condition within a Thread | CWE-416 CWE-416: Use After Free | CWE-476 CWE-476: NULL Pointer Dereference | CWE-826 CWE-826: Premature Release of Resource During Expected Lifetime

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Tukaani-project</a>	Xz	affected >= 5.3.3alpha, < 5.8.1	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518-4 PN/DP MFP</a>	affected V3.1.5 * custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518-4 PN/DP MFP</a>	affected V3.1.5 * custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP</a>	affected V3.1.5 * custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP</a>	affected V3.1.5 * custom	Not specified
ADP	<a href="#">Siemens</a>	<a href="#">SIPLUS S7-1500 CPU 1518-4 PN/DP MFP</a>	affected V3.1.5 * custom	Not specified

### References

Reference	Source	Link
<a href="#">tukaani.org/xz/xz-cve-2025-31115.patch</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="#">tukaani.org</a>
<a href="#">cert-portal.siemens.com/productcert/html/ssa-082556.html</a>	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="#">cert-portal.s</a>
<a href="#">github.com/tukaani-project/xz/security/advisories/GHSA-6cc8-p5mm-29w2</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="#">github.com</a>
<a href="#">github.com/tukaani-project/xz/commit/d5a2ffe41bb77b918a8c96084885d4dbe4b...</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="#">github.com</a>
<a href="#">www.openwall.com/lists/oss-security/2025/04/03/3</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.openv</a>
<a href="#">www.openwall.com/lists/oss-security/2025/04/03/2</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.openv</a>
<a href="#">www.openwall.com/lists/oss-security/2025/04/03/1</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.openv</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.or</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)