Use-after-free in lzma.LZMADecompressor, bz2.BZ2Decompressor, and gzip.GzipFile after re-use under memory pressure

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6100
State	PUBLISHED
Assigner	PSF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 18:16:31 UTC
Updated	2026-04-17 15:18:16 UTC
Description	Use-after-free (UAF) was possible in the `lzma.LZMADecompressor`, `bz2.BZ2Decompressor`, and `gzip.GzipFile` when a

Risk And Classification

Primary CVSS: v4.0 9.1 CRITICAL from cna@python.org

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000660000 probability, percentile 0.203230000 (date 2026-04-18)

Problem Types: CWE-416 | CWE-787 | CWE-416 CWE-416 Use after free | CWE-787 CWE-787 Out-of-bounds write

Version	Source	Type	Score	Severity	Vector
4.0	cna@python.org	Secondary	9.1	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:X/C.
4.0	CNA	CVSS	9.1	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/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/MSC:X/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	Python Software Foundation	CPython	affected 3.15.0 python	Not specified

References

Reference	Source	Link
github.com/python/cpython/issues/148395	cna@python.org	github.c
github.com/python/cpython/pull/148396	cna@python.org	github.c
www.openwall.com/lists/oss-security/2026/04/13/10	af854a3a-2127-422b-91ae-364da2661108	www.op
github.com/python/cpython/commit/c3cf71c3366fe49acb776a639405c0eea6169c20	cna@python.org	github.c
github.com/python/cpython/commit/8fc66aef6d7b3ae58f43f5c66f9366cc8cbbfcd2	cna@python.org	github.c
github.com/python/cpython/commit/6a5f79c8d7bbf22b083b240910c7a8781a59437d	cna@python.org	github.c
github.com/python/cpython/commit/e20c6c9667c99ecaab96e1a2b3767082841ffc8b	cna@python.org	github.c
mail.python.org/archives/list/security-announce@python.org/thread/HTWB2Z6KT5Q...	cna@python.org	mail.pyt
github.com/python/cpython/commit/47128e64f98c3a20271138a98c2922bea2a3ee0e	cna@python.org	github.c
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Ryan Hileman (en)

CNA: Stan Ulbrych (en)

CNA: Seth Larson (en)

CNA: Stan Ulbrych (en)

CNA: Ryan Hileman (en)

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