WebSocket permessage-deflate inflate has no output-size cap in bandit

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

Summary

CVE	CVE-2026-39804
State	PUBLISHED
Assigner	EEF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 21:16:16 UTC
Updated	2026-05-02 02:16:00 UTC
Description	Allocation of Resources Without Limits or Throttling vulnerability in mtrudel bandit allows unauthenticated remote denial of s

Risk And Classification

Primary CVSS: v4.0 8.2 HIGH from 6b3ad84c-e1a6-4bf7-a703-f496b71e49db

CVSS:4.0/AV:N/AC:L/AT:P/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-770 | CWE-770 CWE-770 Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
4.0	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	Secondary	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:I
4.0	CNA	CVSS	8.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:I

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

ntegrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/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/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	Mtrudel	Bandit	affected 0.5.9 1.11.0 semver	Not specified
CNA	Mtrudel	Bandit	affected da4027cff7d2b80319e76fe7a32f84beceec490a 1.11.0 git	Not specified

References

Reference	Source	Link
github.com/mtrudel/bandit/commit/8156921a51e684a951221da7bc30a70a022f722e	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	github.com
github.com/mtrudel/bandit/security/advisories/GHSA-frh3-6pv6-rc8j	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
osv.dev/vulnerability/EEF-CVE-2026-39804	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	osv.dev
cna.erlef.org/cves/CVE-2026-39804.html	6b3ad84c-e1a6-4bf7-a703-f496b71e49db	cna.erlef.o
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

Vendor Comments And Credit

Discovery Credit

CNA: Peter Ullrich (en)

Additional Advisory Data

Workarounds

CNA: Do not pass compress: true to WebSockAdapter.upgrade/4. Omitting this option (or setting it to false) prevents permessage-deflate from being negotiated, so the inflate path is never reached.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**