



Unfurl < 2026.04 - Denial of Service via Unbounded zlib Decompression

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

Summary

CVE	CVE-2026-40036
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 22:16:24 UTC
Updated	2026-04-08 22:16:24 UTC
Description	Unfurl before 2026.04 contains an unbounded zlib decompression vulnerability in parse_compressed.py that allows remote

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from disclosure@vulncheck.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

Problem Types: CWE-409 | CWE-770 | CWE-770 CWE-770 Allocation of Resources Without Limits or Throttling | CWE-409 CWE-409 Improper Handling of Highly Compressed Data (Data Amplification)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.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
4.0	CNA	CVSS	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
3.1	disclosure@vulncheck.com	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

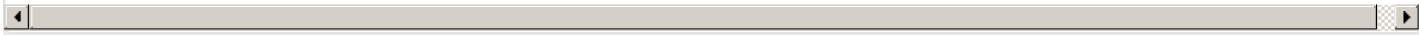
None

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



CVSS v3.1 Breakdown

Attack Vector
Network
Attack Complexity
Low
Privileges Required
None
User Interaction
None
Scope
Unchanged
Confidentiality
None
Integrity
None
Availability
High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Obsidianforensics	Unfurl	affected 2026.04 semver	Not specified

References

Reference	Source	Link	Tag
github.com/obsidianforensics/unfurl/releases/tag/v2026.04	disclosure@vulncheck.com	github.com	
www.vulncheck.com/advisories/dfir-unfurl-denial-of-service-via-unbounded-zlib-d...	disclosure@vulncheck.com	www.vulncheck.com	
github.com/obsidianforensics/unfurl/security/advisories/GHSA-h5qv-qjv4-pc5m	disclosure@vulncheck.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

Vendor Comments And Credit

Discovery Credit

CNA: Mobasi Security Team (en)

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