OSGeo gdal SWapi.c SWnentries heap-based overflow

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

Summary

CVE	CVE-2026-8086
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-07 19:16:03 UTC
Updated	2026-05-08 19:04:48 UTC
Description	A vulnerability was identified in OSGeo gdal up to 3.13.0dev-4. This issue affects the function SWnentries of the file frmts/h

Risk And Classification

Primary CVSS: v4.0 1.9 LOW from cna@vuldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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: 0.000120000 probability, percentile 0.018270000 (date 2026-05-08)

Problem Types: CWE-119 | CWE-122 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	1.9	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	5.3	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Osgeo	Gdal	3.13.0	beta1	All	All
Application	Osgeo	Gdal	3.13.0	beta2	All	All
Application	Osgeo	Gdal	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OSGeo	Gdal	affected 3.13.0dev-4	Not specified
CNA	OSGeo	Gdal	unaffected 3.12.4RC1	Not specified

References

Reference	Source	Link
github.com/biniamf/pocs/tree/main/gdal-swinqdims_bof	cna@vuldb.com	github.com
vuldb.com/submit/808038	134c704f-9b21-4f2e-91b3-4a467353bcc0	vuldb.com
github.com/OSGeo/gdal/commit/9491e794f1757f08063ea2f7a274ad2994afa636	cna@vuldb.com	github.com
vuldb.com/vuln/361839/cti	cna@vuldb.com	vuldb.com
github.com/OSGeo/gdal/issues/14356	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
vuldb.com/vuln/361839	cna@vuldb.com	vuldb.com
github.com/OSGeo/gdal/releases/tag/v3.12.4RC1	cna@vuldb.com	github.com
github.com/OSGeo/gdal	cna@vuldb.com	github.com

github.com/OSGeo/gdal/pull/14361	cna@vuldb.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: biniam (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-05-07T00:00:00.000Z	Advisory disclosed
CNA	2026-05-07T02:00:00.000Z	VulDB entry created
CNA	2026-05-07T14:39:32.000Z	VulDB entry last update

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