AdSanity < 1.8.2 - Authenticated Arbitrary File Upload

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

Summary

CVE	CVE-2022-4949
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-07 02:15:15 UTC
Updated	2026-04-08 19:17:58 UTC
Description	The AdSanity plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'ajax_uplo

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.086270000 probability, percentile 0.924340000 (date 2026-04-09)

Problem Types: CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adsanityplugin	Adsanity	All	All	All	All
Operating System	Xen	Xen	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Httpsadsanityplugin.com	AdSanity	affected 1.8.2 semver	Not specified

References

Reference	Source
Critical vulnerability in WordPress AdSanity plugin. – NinTechNet	af854a3
xenbits.xen.org/xsa/advisory-443.html	af854a3
oss-security - Xen Security Advisory 443 v4 (CVE-2023-34325,CVE-2022-4949) - Multiple vulnerabilities in libfsimage disk handling	af854a3
AdSanity < 1.8.2 - Authenticated Arbitrary File Upload	af854a3
CVE Program record	CVE.O
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Jerome Bruandet (en)

Additional Advisory Data

Source	Time	Event
CNA	2022-01-25T00:00:00.000Z	Disclosed

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