



Essential Real Estate <= 4.3.5 - Authenticated (Subscriber+) Arbitrary File Upload

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

Summary

CVE	CVE-2023-6827
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-15 08:15:46 UTC
Updated	2026-04-08 18:18:43 UTC
Description	The Essential Real Estate plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation c

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

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	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:H/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

High

Integrity

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	G5plus	Essential Real Estate	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	G5theme	Essential Real Estate	affected 4.3.5 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/3009780/essential-real-estate	af854a3a-2127-422b-91ae-364da2661108	plug
plugins.trac.wordpress.org/browser/essential-real-estate/tags/4.3.5/lib/smart-framework/...	af854a3a-2127-422b-91ae-364da2661108	plug
www.wordfence.com/threat-intel/vulnerabilities/id/8bb2ce22-077b-41dd-a2ff-cc1db...	af854a3a-2127-422b-91ae-364da2661108	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

Vendor Comments And Credit

Discovery Credit

CNA: István Márton (en)

Additional Advisory Data

Source	Time	Event
CNA	2023-12-12T00:00:00.000Z	Discovered
CNA	2023-12-12T00:00:00.000Z	Vendor Notified
CNA	2023-12-14T00:00:00.000Z	Disclosed

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

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](#)