



# JetWidgets for Elementor <= 1.0.12 - Cross-Site Request Forgery to Settings Update

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

## Summary

<b>CVE</b>	CVE-2023-0086
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-05 17:15:09 UTC
<b>Updated</b>	2026-04-08 18:17:40 UTC
<b>Description</b>	The JetWidgets for Elementor plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and inclu

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
3.1	security@wordfence.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Crocoblock	Jetwidgets For Elementor	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Jetmonsters	JetWidgets For Elementor	affected 1.0.12 semver	Not specified

### References

Reference	Source	Link
JetWidgets for Elementor <= 1.0.12 - Cross-Site Request Forgery to Settings Update	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.wordfence.com">www.wordfence.com</a>
<a href="http://www.wordfence.com/threat-intel/vulnerabilities/id/8de3d3c7-bde2-4455-8d60-20307...">www.wordfence.com/threat-intel/vulnerabilities/id/8de3d3c7-bde2-4455-8d60-20307...</a>	security@wordfence.com	<a href="http://www.wordfence.com">www.wordfence.com</a>
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	<a href="http://plugins.trac.wordpress.org">plugins.trac.wordpress.org</a>
<a href="http://plugins.trac.wordpress.org/changeset">plugins.trac.wordpress.org/changeset</a>	security@wordfence.com	<a href="http://plugins.trac.wordpress.org">plugins.trac.wordpress.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** Chloe Chamberland (en)

**CNA:** Wordfence (en)

### Additional Advisory Data

Source	Time	Event
CNA	2023-01-04T00:00:00.000Z	Disclosed

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)