



FreeMind WP Browser <= 1.2 - Cross-Site Request Forgery to Cross-Site Scripting

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

Summary

CVE	CVE-2022-2443
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-07-18 17:15:09 UTC
Updated	2026-04-08 19:17:51 UTC
Description	The FreeMind WP Browser plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and includi

Risk And Classification

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

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

EPSS: 0.002180000 probability, percentile 0.444100000 (date 2026-04-08)

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	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/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:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freemind Wp Browser Project	Freemind Wp Browser	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Kusbandono	FreeMind WP Browser	affected 1.2 semver	Not specified

References

Reference	Source	Link
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.trac
Vulnerability Advisories - Wordfence	af854a3a-2127-422b-91ae-364da2661108	www.wordf
FreeMind WP Browser <= 1.2 - Cross-Site Request Forgery to Cross-Site Scripting	af854a3a-2127-422b-91ae-364da2661108	www.wordf
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go



Vendor Comments And Credit

Discovery Credit

CNA: Kenya Uematsu (en)

Additional Advisory Data

Source	Time	Event
CNA	2022-07-05T00:00:00.000Z	Disclosed

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

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