



Easy Social Feed <= 6.5.4 - Cross-Site Request Forgery

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

Summary

CVE	CVE-2024-1214
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-21 02:51:38 UTC
Updated	2026-04-08 19:20:35 UTC
Description	The Easy Social Feed – Social Photos Gallery – Post Feed – Like Box plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) via the Like Box widget. An attacker can exploit this vulnerability to perform actions on behalf of the authenticated user, such as changing the user's profile picture or password, or deleting posts. This vulnerability affects Easy Social Feed versions 6.5.4 and earlier.

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from security@wordfence.com

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

EPSS: 0.001020000 probability, percentile 0.280590000 (date 2026-04-09)

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

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Easysocialfeed	Easy Social Feed	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Sjaved	Easy Social Feed Social Photos Gallery And Post Feed For WordPress	affected 6.5.4 semver	Not specified

References

Reference	Source
www.wordfence.com/threat-intel/vulnerabilities/id/aaf62045-b9ce-40d7-92b3-7ab68...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/browser/easy-facebook-likebox/trunk/facebook/admin/class-easy...	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Eldar Zeynalli (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-03-12T00:00:00.000Z	Disclosed

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). 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