



ProfilePress <= 4.15.1 - Authenticated (Contributor+) Stored Cross-Site Scripting via profilepress-edit-profile Shortcode

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

Summary

CVE CVE-2024-1806**State** PUBLISHED**Assigner** Wordfence**Source Priority** CVE Program / NVD first with legacy fallback**Published** 2024-03-13 16:15:27 UTC**Updated** 2026-04-08 19:20:52 UTC**Description** The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePr

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov**CVSS:** 3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N**EPSS:** 0.002600000 probability, percentile 0.493410000 (date 2026-04-12)**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Properfraction	Profilepress	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product
CNA	Properfraction	Paid Membership Plugin Ecommerce User Registration Form Login Form User Profile Restrict Content ProfilePress

References

Reference	Source	L
www.wordfence.com/threat-intel/vulnerabilities/id/d3b9d0ab-d785-4e93-9ab8-f7567...	af854a3a-2127-422b-91ae-364da2661108	w
plugins.trac.wordpress.org/browser/wp-user-avatar/tags/4.15.0/src/ShortcodeParser/EditPr...	af854a3a-2127-422b-91ae-364da2661108	p
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	p
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

Vendor Comments And Credit

Discovery Credit

CNA: wesley (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-02-23T00:00:00.000Z	Disclosed

Legacy QID Mappings

150848 WordPress ProfilePress Plugin: Stored Cross-Site Scripting Vulnerability (CVE-2024-1806)

© [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](#) 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](#)