



User Profile Picture <= 2.6.1 - Authenticated (Author+) Insecure Direct Object Reference to Profile Picture Update

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

Summary

CVE	CVE-2024-5639
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-06-21 07:15:10 UTC
Updated	2026-04-08 17:19:05 UTC
Description	The User Profile Picture plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and in

Risk And Classification

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

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

Problem Types: CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cozmoslabs	User Profile Picture	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cozmoslabs	User Profile Picture	affected 2.6.1 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/metronet-profile-picture/tags/2.6.1/metronet-profile-...	af854a3a-2127-422b-91ae-364da2661108	plugi
plugins.trac.wordpress.org/browser/metronet-profile-picture/tags/2.6.1/metronet-profile-...	af854a3a-2127-422b-91ae-364da2661108	plugi
plugins.trac.wordpress.org/changeset/3105132	af854a3a-2127-422b-91ae-364da2661108	plugi
www.wordfence.com/threat-intel/vulnerabilities/id/01a3b9ba-b18a-48d9-8365-d10f7...	af854a3a-2127-422b-91ae-364da2661108	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

Vendor Comments And Credit

Discovery Credit

CNA: Stephanie Walters (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-06-20T00:00:00.000Z	Disclosed

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

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