WP To Do <= 1.3.0 - Cross-Site Request Forgery via wptodo_addcomment

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-3943
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-30 05:15:55 UTC
Updated	2026-04-08 18:21:37 UTC
Description	The WP To Do plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.0.

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/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	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
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

ntegrity

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	Delower	Wp To Do	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Delower186	WP To Do	affected 1.3.0 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.tra
plugins.trac.wordpress.org/browser/wp-todo/trunk/inc/Base/Model.php	af854a3a-2127-422b-91ae-364da2661108	plugins.tra
www.wordfence.com/threat-intel/vulnerabilities/id/406f6bd7-f57f-4725-a36f-9846a...	af854a3a-2127-422b-91ae-364da2661108	www.word
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

Vendor Comments And Credit

Discovery Credit

CNA: Benedictus Jovan (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-05-29T15:54:21.000Z	Disclosed

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

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