



Ultimate Dashboard <= 3.8.14 - Cross-Site Request Forgery to Module Activation/Deactivation

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2026-3140
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 12:16:15 UTC
Updated	2026-05-01 15:26:24 UTC
Description	The Ultimate Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and includi

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: 0.000050000 probability, percentile 0.002320000 (date 2026-05-05)

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

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	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	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

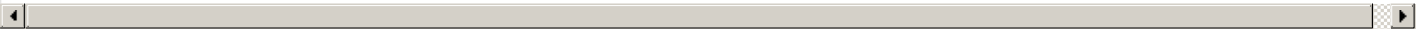
Integrity

Low

Availability

None

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



Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Davidvongries	Ultimate Dashboard Custom WordPress Dashboard	affected 3.8.14 semver	Not specified

References		
Reference	Source	Link
plugins.trac.wordpress.org/browser/ultimate-dashboard/trunk/modules/feature/class-featur...	security@wordfence.com	plugins.trac.wordpr
plugins.trac.wordpress.org/changeset/3479396	security@wordfence.com	plugins.trac.wordpr
www.wordfence.com/threat-intel/vulnerabilities/id/bbcd70f-77db-48ab-ae23-c46ca...	security@wordfence.com	www.wordfence.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



Vendor Comments And Credit
Discovery Credit
CNA: Nabil Irawan (en)

Additional Advisory Data		
Source	Time	Event
CNA	2026-03-10T13:16:23.000Z	Vendor Notified
CNA	2026-04-30T00:00:00.000Z	Disclosed

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