



Supreme Modules Lite – Divi Theme, Extra Theme and Divi Builder <= 2.5.51 - Authenticated (Contributor+) Stored Cross-Site Scripting

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

Summary

CVE	CVE-2024-5501
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-06-01 06:15:09 UTC
Updated	2026-04-08 18:22:05 UTC
Description	The Supreme Modules Lite – Divi Theme, Extra Theme and Divi Builder plugin for WordPress is vulnerable to Stored Cross

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from security@wordfence.com

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

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	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

None

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Divisupreme	Supreme Modules Lite Divi Theme Extra Theme And Divi Builder	affected 2.5.51 semver	Not specified

References

Reference	Source
plugins.trac.wordpress.org/browser/supreme-modules-for-divi/trunk/includes/modules/Butto...	af854a3a-2127-422b-91ae-364da2661108
www.wordfence.com/threat-intel/vulnerabilities/id/6543e6e2-e052-466e-ad19-656fd...	af854a3a-2127-422b-91ae-364da2661108
plugins.trac.wordpress.org/changeset/3095671	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Ngô Thiên An (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-05-31T00:00:00.000Z	Disclosed

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