



The7 <= 14.3.2 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode 'link' Parameter

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

Summary

CVE	CVE-2026-6646
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-15 07:16:20 UTC
Updated	2026-05-15 07:16:20 UTC
Description	The The7 theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'dt_default_button' shortcode in all versi

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	Primary	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

Severity: **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	Dream-Theme	The7 Website And ECommerce Builder For WordPress	affected 14.3.2 semver	Not specified

References			
Reference	Source	Link	
the7.io/changelog	security@wordfence.com	the7.io	
plugins.trac.wordpress.org/browser/dt-the7/tags/14.2.2/inc/shortcodes/includes/default-b...	security@wordfence.com	plugins.trac.wordpress.org/browser/dt-the7/tags/14.2.2/inc/shortcodes/includes/default-b...	
www.wordfence.com/threat-intel/vulnerabilities/id/082f810c-d55e-4190-908c-c7dd9...	security@wordfence.com	www.wordfence.com/threat-intel/vulnerabilities/id/082f810c-d55e-4190-908c-c7dd9...	
plugins.trac.wordpress.org/browser/dt-the7/tags/14.2.2/inc/shortcodes/includes/default-b...	security@wordfence.com	plugins.trac.wordpress.org/browser/dt-the7/tags/14.2.2/inc/shortcodes/includes/default-b...	
plugins.trac.wordpress.org/browser/dt-the7/trunk/inc/helpers/html-helpers.php	security@wordfence.com	plugins.trac.wordpress.org/browser/dt-the7/trunk/inc/helpers/html-helpers.php	
plugins.trac.wordpress.org/browser/dt-the7/tags/14.2.2/inc/helpers/html-helpers.php	security@wordfence.com	plugins.trac.wordpress.org/browser/dt-the7/tags/14.2.2/inc/helpers/html-helpers.php	
plugins.trac.wordpress.org/browser/dt-the7/trunk/inc/shortcodes/includes/default-button/...	security@wordfence.com	plugins.trac.wordpress.org/browser/dt-the7/trunk/inc/shortcodes/includes/default-button/...	
plugins.trac.wordpress.org/browser/dt-the7/trunk/inc/shortcodes/includes/default-button/...	security@wordfence.com	plugins.trac.wordpress.org/browser/dt-the7/trunk/inc/shortcodes/includes/default-button/...	
CVE Program record	CVE.ORG	www.cve.org	
NVD vulnerability detail	NVD	nvd.nist.gov	

Vendor Comments And Credit

Discovery Credit

CNA: João Pedro S Alcântara (Kinorth) (en)

Additional Advisory Data		
Source	Time	Event
CNA	2026-04-20T05:16:33.000Z	Vendor Notified
CNA	2026-05-14T00:00:00.000Z	Disclosed

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

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