Buzz Comments <= 0.9.4 - Authenticated (Administrator+) Stored Cross-Site Scripting via 'Custom Buzz Avatar' Setting

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

Summary

CVE	CVE-2026-6041
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 09:16:26 UTC
Updated	2026-04-22 09:16:26 UTC
Description	The Buzz Comments plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Custom Buzz Avatar' (buzz_

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from security@wordfence.com

CVSS:3.1/AV:N/AC:H/PR:H/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	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mixer2	Buzz Comments	affected 0.9.4 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/buzz-comments/trunk/admin.tpl.php	security@wordfence.com	plugins.trac.wordpress.or
www.wordfence.com/threat-intel/vulnerabilities/id/1516ebe7-4d16-4e97-9baa-bc585...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/buzz-comments/trunk/buzzComments_class.php	security@wordfence.com	plugins.trac.wordpress.or
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Muhammad Nur Ibnu Hubab (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-21T19:03:15.000Z	Disclosed

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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 registred 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**