



# Bold Page Builder <= 4.8.8 - Authenticated (Contributor+) Stored Cross-Site Scripting via Widget URL Attribute

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

## Summary

<b>CVE</b>	CVE-2024-3266
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-04-09 19:15:40 UTC
<b>Updated</b>	2026-04-08 17:18:42 UTC
<b>Description</b>	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL attribute of widgets in

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:L/UI:R/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	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
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

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Bold-themes</a>	<a href="#">Bold Page Builder</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Boldthemes</a>	<a href="#">Bold Page Builder</a>	affected 4.8.8 semver	Not specified

### References

Reference	Source	Link
<a href="http://www.wordfence.com/threat-intel/vulnerabilities/id/21fed5a3-1bb2-4581-95b4-badff...">www.wordfence.com/threat-intel/vulnerabilities/id/21fed5a3-1bb2-4581-95b4-badff...</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.wordfence.com">www.wordfence.com</a>
<a href="https://plugins.trac.wordpress.org/changeset/3064413/bold-page-builder">plugins.trac.wordpress.org/changeset/3064413/bold-page-builder</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://plugins.trac.wordpress.org">plugins.trac.wordpress.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Discovery Credit

**CNA:** wesley (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-04-03T00:00:00.000Z	Vendor Notified
CNA	2024-04-05T00:00:00.000Z	Disclosed

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)