



# Avada <= 6.2.2 - Authenticated (Contributor+) Cross-Site Scripting

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

## Summary

<b>CVE</b>	CVE-2020-36711
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-07 02:15:11 UTC
<b>Updated</b>	2026-04-08 18:17:08 UTC
<b>Description</b>	The Avada theme for WordPress is vulnerable to Stored Cross-Site Scripting via the update_layout function in versions up to 6.2.2. An authenticated user with contributor or higher privileges can inject arbitrary HTML and JavaScript into the site's layout, which is then rendered to all users. This can be used to steal session cookies, perform actions on behalf of the user, or deface the site.

## 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

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	Theme-fusion	Avada	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ThemeFusion	Avada Website Builder For WordPress WooCommerce	affected 6.2.3 semver	Not specified

References

Reference	Source	Link
Avada WordPress Theme fixed multiple vulnerabilities. – NinTechNet	af854a3a-2127-422b-91ae-364da2661108	<a href="http://blog.nintech.net">blog.nintech.net</a>
Security Fix Added in 6.2.3 - ThemeFusion   Avada Website Builder	af854a3a-2127-422b-91ae-364da2661108	<a href="http://theme-fusion.com">theme-fusion.com</a>
Avada <= 6.2.2 - Authenticated (Contributor+) Cross-Site Scripting	af854a3a-2127-422b-91ae-364da2661108	<a href="http://www.wordfence.com">www.wordfence.com</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: Jerome Bruandet (en)**

Additional Advisory Data

Source	Time	Event
CNA	2020-04-24T00:00:00.000Z	Disclosed

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

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)