



# CVE-2018-20838

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

## Summary

<b>CVE</b>	CVE-2018-20838
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-05-13 05:29:00 UTC
<b>Updated</b>	2019-05-14 21:29:00 UTC
<b>Description</b>	ampforwp_save_steps_data in the AMP for WP plugin before 0.9.97.21 for WordPress allows stored XSS.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Magazine3</a>	<a href="#">Amp For Wp</a>	All	All	All	All
Application	<a href="#">Magazine3</a>	<a href="#">Amp For Wp</a>	All	All	All	All

## References

Reference	Source	Link	Tags
XSS Injection Campaign Exploits WordPress AMP Plugin	MISC	<a href="http://www.wordfence.com">www.wordfence.com</a>	Exploit, Third P
403 Forbidden	MISC	<a href="http://plugins.trac.wordpress.org">plugins.trac.wordpress.org</a>	Release Notes
Critical Security Issues has been fixed in 0.9.97.20 version! – AMP for WordPress	MISC	<a href="http://ampforwp.com">ampforwp.com</a>	
AMP for WP – Accelerated Mobile Pages – WordPress plugin   WordPress.org	MISC	<a href="http://wordpress.org">wordpress.org</a>	Release Notes
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

No vendor comments have been submitted for this CVE.

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

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 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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**