



# CVE-2018-20150

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-20150
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-14 20:29:00 UTC
<b>Updated</b>	2019-03-04 14:21:00 UTC
<b>Description</b>	In WordPress before 4.9.9 and 5.x before 5.0.1, crafted URLs could trigger XSS for certain use cases involving plugins.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Wordpress</a>	<a href="#">Wordpress</a>	All	All	All	All
Application	<a href="#">Wordpress</a>	<a href="#">Wordpress</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4401-1 wordpress	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	Third Party Adviso
Version 4.9.9   WordPress.org	MISC	<a href="http://codex.wordpress.org">codex.wordpress.org</a>	Product, Vendor A
WordPress Prior to 5.0.1 Multiple Security Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Adviso
WordPress 5.0.1 Security Release	MISC	<a href="http://wordpress.org">wordpress.org</a>	Release Notes, Ve
[SECURITY] [DLA 1673-1] wordpress security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Mailing List, Third
Version 5.0.1   WordPress.org	MISC	<a href="http://wordpress.org">wordpress.org</a>	Release Notes, Ve
WordPress plugs bug that led to Google indexing some user passwords   ZDNet	MISC	<a href="http://www.zdnet.com">www.zdnet.com</a>	Press/Media Cove
KSES: Make the URI attributes DRY. · WordPress/WordPress@fb3c6ea · GitHub	MISC	<a href="http://github.com">github.com</a>	Patch, Third Party
WordPress <= 5.0 - Cross Site Scripting (XSS) that could affect plugins	MISC	<a href="http://www.inh.com">www.inh.com</a>	Vendor Advisory

wordpress <= 3.0 - Cross-Site Scripting (XSS) that could affect plugins	MISC	<a href="http://wpsvulnlab.com">wpsvulnlab.com</a>	Vendor Advisory
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, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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 registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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)