



CVE-2019-20204

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

Summary

CVE	CVE-2019-20204
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-02 14:16:00 UTC
Updated	2023-01-20 20:51:00 UTC
Description	The Postie plugin 1.9.40 for WordPress allows XSS, as demonstrated by a certain payload with jaVaScRipt:/* at the beginni

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postieplugin	Postie	All	All	All	All

References

Reference	Source	Link
Exploiting-Postie-WordPress-Plugin-/README.md at master · V1n1v131r4/Exploiting-Postie-WordPress-Plugin- · GitHub	MISC	github
WordPress › WordPress Plugins	MISC	worc
WordPress Postie 1.9.40 Cross Site Scripting ≈ Packet Storm	MISC	pack
Postie Plugin Blog via email with WordPress	MISC	post
Postie <= 1.9.40 - Post Submission Spoofing & Stored XSS	MISC	wpvi
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

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 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](#)

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