



CVE-2017-5491

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

Summary

CVE	CVE-2017-5491
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-15 02:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	wp-mail.php in WordPress before 4.7.1 might allow remote attackers to bypass intended posting restrictions via a spoofed r

Risk And Classification

Problem Types: CWE-1188

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	All	All	All	All

References

Reference
oss-security - Re: CVE Request: Wordpress: 8 security issues in 4.7
Mail: Disable wp-mail.php when `mailserver_url` is mail.example.com. · WordPress/WordPress@061e878 · GitHub
Version 4.7.1 « WordPress Codex
WordPress Prior to 4.7.1 Security Bypass Vulnerability
WordPress Bugs Let Remote Users Conduct Cross-Site Scripting and Cross-Site Request Forgery Attacks and Obtain Potentially Sensitive In
WordPress <= 4.7 - Post via Email Checks mail.example.com by Default
Debian -- Security Information -- DSA-3779-1 wordpress
WordPress 4.7.1 Security and Maintenance Release
CVE Program record
NVD vulnerability detail

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](#)