



CVE-2016-10033

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

Summary

CVE	CVE-2016-10033
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-30 19:59:00 UTC
Updated	2021-09-30 16:30:00 UTC
Description	The mailSend function in the isMail transport in PHPMailer before 5.2.18 might allow remote attackers to pass extra param

Risk And Classification

EPSS: 0.944650000 probability, percentile 0.999960000 (date 2026-04-01)

CISA KEV: Listed on 2025-07-07; due 2025-07-28; ransomware use Unknown

Problem Types: CWE-77

CISA Known Exploited Vulnerability

Vendor	PHP
Product	PHPMailer
Name	PHPMailer Command Injection Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products. For more information, please see: https://github.com/PHPMailer/PHPMailer/releases/tag/v5.2.18 ; https://github.com/advisories/GHSA-5f37-gxvh-23v6 ; https://nvd.nist.gov/vuln/detail/CVE-2016-10033

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joomla	Joomla!	All	All	All	All
Application	Phpmailer Project	Phpmailer	All	All	All	All
Application	Phpmailer Project	Phpmailer	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference

[Release PHPMailer 5.2.18 · PHPMailer/PHPMailer · GitHub](#)

[SecurityFocus](#)

[CVE-2016-10033 PHPMailer Sendmail Argument Injection | Rapid7](#)

[PHPMailer < 5.2.20 - Remote Code Execution](#)

[PHPMailer Remote Code Execution ≈ Packet Storm](#)

[About the CVE 2016 10033 and CVE 2016 10045 vulnerabilities · PHPMailer/PHPMailer Wiki · GitHub](#)

[WordPress Plugin PHPMailer 4.6 - Host Header Command Injection \(Metasploit\) - PHP remote Exploit](#)

[PHPMailer < 5.2.20 with Exim MTA - Remote Code Execution - PHP webapps Exploit](#)

[PHPMailer Input Validation Flaw Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker](#)

[PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln](#)

[Full Disclosure: PHPMailer < 5.2.18 Remote Code Execution \[CVE-2016-10033\]](#)

[PHPMailer CVE-2016-10033 Remote Code Execution Vulnerability](#)

[PHPMailer 3rd party library -- DRUPAL-SA-PSA-2016-004 | Drupal.org](#)

[PHPMailer Sendmail Argument Injection ≈ Packet Storm](#)

[PHPMailer < 5.2.18 - Remote Code Execution \(PHP\)](#)

[PHPMailer < 5.2.20 / SwiftMailer < 5.4.5-DEV / Zend Framework / zend-mail < 2.4.11 - 'AIO' 'PwnScriptum' Remote Code Execution - PHP we](#)

[WordPress 4.6 - Unauthenticated Remote Code Execution](#)

[PHPMailer < 5.2.18 - Remote Code Execution \(Bash\)](#)

[Vanilla Forums < 2.3 - Remote Code Execution - PHP remote Exploit](#)

[\[20161205\] - PHPMailer Security Advisory](#)

[PHPMailer < 5.2.18 - Remote Code Execution \(Python\) - PHP webapps Exploit](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

[CISA Known Exploited Vulnerabilities catalog](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199517](#) Ubuntu Security Notification for PHPMailer Vulnerabilities (USN-5956-1)

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](#)