

# CVE-2016-10033

## PHPMailer Command Injection Vulnerability

Exigent

CISA KEV since Jul 7, 2025

Actively exploited

Public exploit module (Metasploit)

The mailSend function in the isMail transport in PHPMailer before 5.2.18 might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code via a \" (backslash double quote) in a crafted Sender property.

|                                                            |                                                          |                                                                   |                                                                                            |
|------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>88</b>/100</p> <p>Immediate priority</p> | <p>CVSS V3.1</p> <p><b>9.8</b></p> <p>Critical · NVD</p> | <p>EPSS</p> <p><b>0.997</b></p> <p>99.95th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Jul 28, 2025</b></p> <p>KEV since 2025 · listed over a year</p> |
|------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                             |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|---------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild          |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | Added to CISA KEV within the last two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.997 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable               |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 9.8                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                         |

### Remediation

**Out-of-band / urgent** Patch or fixed version identified

**CISA 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. **CISA note:** This vulnerability could affect an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE             | AFFECTED          | FIXED IN                | SOURCE |
|---------------------|-------------------|-------------------------|--------|
| phpmailer/phpmailer | ≥ 5.0.0, < 5.2.18 | 5.2.18                  | GitHub |
| phpmailer           | < 5.2.18          | no fixed version listed | NVD    |
| wordpress           | ≤ 4.7             | no fixed version listed | NVD    |
| joomla!             | ≥ 1.5.0 ≤ 3.6.5   | no fixed version listed | NVD    |

### Sources

|                        |                                                                                                                               |                        |                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://github.com/PHPMailer/PHPMailer/releases/tag/v5.2.18">github.com/PHPMailer/PHPMailer/releases/tag/v5.2.18</a> | <b>GitHub advisory</b> | <a href="https://github.com/advisories/GHSA-5f37-gxvh-23v6">github.com/advisories/GHSA-5f37-gxvh-23v6</a>                                 |
| <b>NVD</b>             | <a href="https://nvd.nist.gov/vuln/detail/CVE-2016-10033">nvd.nist.gov/vuln/detail/CVE-2016-10033</a>                         | <b>CISA KEV</b>        | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                   |
| <b>ENISA EUVD</b>      | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2020-0331">euvd.enisa.europa.eu/vulnerability/EUVD-2020-0331</a>     | <b>Current data</b>    | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2016-10033">evulnable.com/vulnerability-management/cve/CVE-2016-10033</a> |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.