



# CVE-2020-13625

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

## Summary

<b>CVE</b>	CVE-2020-13625
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-08 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:16:00 UTC
<b>Description</b>	PHPMailer before 6.1.6 contains an output escaping bug when the name of a file attachment contains a double quote char

## Risk And Classification

**Problem Types:** CWE-116

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	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
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">Phpmailer Project</a>	<a href="#">Phpmailer</a>	All	All	All	All
Application	<a href="#">Phpmailer Project</a>	<a href="#">Phpmailer</a>	All	All	All	All

## References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:1106-1: moderate: Security update f	SUSE	<a href="#">lists.opensuse.org</a>
[security-announce] openSUSE-SU-2020:1060-1: moderate: Security update f	SUSE	<a href="#">lists.opensuse.org</a>
Release PHPMailer 6.1.6 · PHPMailer/PHPMailer · GitHub	CONFIRM	<a href="#">github.com</a>
USN-4505-1: PHPMailer vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="#">usn.ubuntu.com</a>
2020-05-26 Insufficient output escaping of attachment names · Advisory · PHPMailer/PHPMailer · GitHub	CONFIRM	<a href="#">github.com</a>
[SECURITY] [DLA 2244-1] libphp-phpmailer security update	MLIST	<a href="#">lists.debian.org</a>
[SECURITY] [DLA 2306-1] libphp-phpmailer security update	MLIST	<a href="#">lists.debian.org</a>

[SECURITY] Fedora 32 Update: php-PHPMailer-5.2.28-2.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.or</a>
[SECURITY] Fedora 31 Update: php-PHPMailer-5.2.28-2.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.or</a>
[SECURITY] Fedora 31 Update: php-PHPMailer-5.2.28-2.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.or</a>
[SECURITY] Fedora 32 Update: php-PHPMailer-5.2.28-2.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.or</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [199517](#) Ubuntu Security Notification for PHPMailer Vulnerabilities (USN-5956-1)
- [501529](#) Alpine Linux Security Update for cacti
- [504593](#) Alpine Linux Security Update for cacti
- [690483](#) Free Berkeley Software Distribution (FreeBSD) Security Update for cacti (cd2dc126-cfe4-11ea-9172-4c72b94353b5)

© [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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)