# 2020-05-26 Insufficient output escaping of attachment names

Low **Synchro** published **GHSA-f7hx-fqxw-rvvj** on May 27, 2020

Package

PHPMailer (Packagist)

| Affected versions | Patched versions |
|---|---|
| <=6.1.5 | 6.1.6 |

Description

### Impact

CWE-116: Incorrect output escaping.

An attachment added like this (note the double quote within the attachment name, which is entirely valid):

```
$mail->addAttachment('/tmp/attachment.tmp', 'filename.html";.jpg');
```

Will result in a message containing these headers:

```
Content-Type: application/octet-stream; name="filename.html";.jpg"
Content-Disposition: attachment; filename="filename.html";.jpg"
```

The attachment will be named `filename.html`, and the trailing `";.jpg"` will be ignored. Mail filters that reject `.html` attachments but permit `.jpg` attachments may be fooled by this.

Note that the MIME type itself is obtained automatically from the *source filename* (in this case `attachment.tmp`, which maps to a generic `application/octet-stream` type), and not the *name* given to the attachment (though these are the same if a separate name is not provided), though it can be set explicitly in other parameters to attachment methods.

### Patches

Patched in PHPMailer 6.1.6 by escaping double quotes within the name using a backslash, as per RFC822 section 3.4.1, resulting in correctly escaped headers like this:

```
Content-Type: application/octet-stream; name="filename.html\";.jpg"
Content-Disposition: attachment; filename="filename.html\";.jpg"
```

### Workarounds

Reject or filter names and filenames containing double quote ( `"` ) characters before passing them to attachment functions such as `addAttachment()`.

### References

CVE-2020-13625.
PHPMailer 6.1.6 release

### For more information

If you have any questions or comments about this advisory:

- Open an issue in the PHPMailer repo

Severity

Low

CVE ID

CVE-2020-13625

Weaknesses

No CWEs