Alpine Linux - Bug #6623

Bug # 6622 (Closed): phpmailer: Remote Code Execution (CVE-2016-10033, CVE-2016-10045)

[3.5] phpmailer: Remote Code Execution (CVE-2016-10033, CVE-2016-10045)

01/04/2017 03:20 PM - Alicha CH

Status:	Closed	**Start date:**	01/04/2017
Priority:	Normal	**Due date:**	
Assignee:	Timo Teräs	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.5.1		
Affected versions:		**Security IDs:**	

Description

CVE-2016-10033:

The mailSend function in the isMail transport in PHPMailer before 5.2.18, when the Sender property is not set,
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 From address.

Fixed In Version:

phpmailer 5.2.18

Reference:

http://seclists.org/oss-sec/2016/q4/750

CVE-2016-10045:

The isMail transport in PHPMailer before 5.2.20, when the Sender property is not set, might allow remote attackers to pass extra parameters
to the mail command and consequently execute arbitrary code by leveraging improper interaction between the escapeshellarg function and
internal escaping performed in the mail function. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-10033.

Fixed in Version:

phpmailer 5.2.20

Reference:

https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10045-Vuln-Patch-Bypass.html

Associated revisions

Revision 66935a2a - 01/12/2017 07:56 AM - Sergei Lukin

main/php5-phpmailer: security fixes #6623

CVE-2016-10033
CVE-2016-10045

Issues were fixed in 5.2.18 and 5.2.20
However, there were major changes between 5.2.4 and 5.2.20
https://github.com/PHPMailer/PHPMailer/blob/master/changelog.md

This upgrade contains patch which is based on 2 commits
containing fix for CVE-2016-10045 and CVE-2016-10033:
https://github.com/PHPMailer/PHPMailer/commit/9743ff5c7ee16e8d49187bd2e11149afb9485eae
https://github.com/PHPMailer/PHPMailer/commit/833c35fe39715c3d01934508987e97af1fbc1ba0
Commits were adjusted to 5.2.4

History

#1 - 01/12/2017 07:57 AM - Sergei Lukin

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:66935a2a80b13056fe0c3f0a127c540f6ea337e1.

#2 - 01/12/2017 02:25 PM - Natanael Copa

- Target version changed from 3.5.0 to 3.5.1

#3 - 01/23/2017 09:36 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed