BOLETÍN DE ALERTA

Boletín Nro.: 2016-15
Fecha de publicación: 29/12/2016
Tema: Vulnerabilidades de Ejecución Remota de Código en PHPMailer

Sistemas afectados:

- PHPMailer < 5.2.20
- Cualquier plugin, framework, CMS u otros que incluyen dicha clase PHP

Descripción:

Hace unos días se descubrió una vulnerabilidad de ejecución remota de código en PHPMailer, una librería de PHP utilizada para envío de correos, que está presente en numerosos sitios web, y que muchas veces viene incluida con CMS y plugins.
La vulnerabilidad se debe a una sanitización inadecuada de los parámetros de la función de envío de correo, la cual puede ser utilizada para ejecutar código remoto en el servidor. La vulnerabilidad puede ser explotada en cualquier servidor en el que se den las siguientes condiciones:

1. La aplicación utiliza isMail(), la función de transporte por defecto que a su vez utiliza la función mail()
2. El parámetro From es obtenido de una entrada de usuario
3. Las propiedades de Sender no son establecidas explícitamente
4. El servidor no ejecuta el servicio de postfix

Al no estar establecida explícitamente las propiedades Sender, éstos se copian de la dirección, la cual es convertida a string y es pasada a la función mail() de PHP como parámetro adicional.
Es posible construir una dirección de correo que cumpla con el formato establecido, pero que además, ejecute código.

La vulnerabilidad fue identificada por CVE-2016-10033, y el día 26/12 se publicó una nueva versión, 5.2.18, y luego la 5.2.19, las cuales pretendían corregir la vulnerabilidad. Sin embargo, el día de ayer se notificó que el parche en realidad no corregía completamente la vulnerabilidad, y que existían maneras de evadir los controles implementados. Esta vulnerabilidad se identificó con CVE-2016-10045. Se ha publicado una nueva versión 5.2.20, y posteriormente 5.2.21 las cuales corrigen esta vulnerabilidad.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Los afectados por el fallo de seguridad de PHPMailer no solo son usuarios, sino que también se pueden contar por varios los CMS que son vulnerables a *exploits* que permiten ejecutar código de forma remota. WordPress, Drupal, Joomla, y muchos otros gestores de contenidos utilizan esta librería para permitir el envío de correos. Muchos plugins también deberán ser actualizados próximamente, de modo a incluir la librería corregida.
A pesar de que el investigador decidió no publicar todos los detalles de la vulnerabilidad, debido al impacto que podría tener en los millones de sitios que no se encuentran actualizados, ya se han desarrollado exploits públicos, lo que aumenta el riesgo de ataque. Se ha descubierto que estas vulnerabilidades ya están siendo explotadas masivamente. un atacante puede utilizar algún componente básico de la web como los formularios de contacto/comentario, formularios de registro, reseteo de contraseñas, o cualquier otro que envíe correos electrónicos para poder comprometer el servidor.

Impacto:
Una explotación exitosa podría permitir a atacantes ejecutar código arbitrario, obteniendo así un control total sobre el servidor web.

Solución:

Actualizar PHPMailer a la última versión, 5.2.21. La misma puede ser obtenida aquí: https://github.com/PHPMailer/PHPMailer
En el caso de que su aplicación web utilice un plugin o componente basado en PHPMailer, el mismo debe ser actualizado, en caso de que el desarrollador del mismo haya publicado una nueva versión que corrija la vulnerabilidad.

Información adicional:

https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-10045-vulnerabilities
https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10033-Vuln.html
https://legalhackers.com/advisories/PHPMailer-Exploit-Remote-Code-Exec-CVE-2016-10045-Vuln-Patch-Bypass.html

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py