BOLETÍN DE ALERTA

Boletín Nro.: 2017-14
Fecha de publicación: 21/09/2017
Tema: Vulnerabilidad OPTIONbleed en Apache

Sistemas afectados:

- Apache Web Server 2.2.x hasta 2.2.34 y 2.4.x hasta 2.4.27.

Descripción:

Se ha descubierto una vulnerabilidad que afectan a Apache Web Server, la cual fue bautizada como OPTIONbleed, a la cual fue asignada el identificador CVE-2017-9798. Se trata de una vulnerabilidad del mal manejo de memoria del tipo *use after free* en Apache HTTP, que permite construir una cabecera Allow corrupta en respuesta a una petición HTTP con el método OPTION. Esta respuesta, además de responder la lista de los métodos permitidos, permite también obtener datos de regiones arbitrarias de la memoria del proceso del servidor, que podría contener información sensible, tanto del propio servidor (contraseñas, por ejemplo), como de los usuarios que lo visitan. Las porciones de memoria que son filtradas varían en cada petición, por lo que puede obtenerse una cantidad arbitraria de datos de memoria.

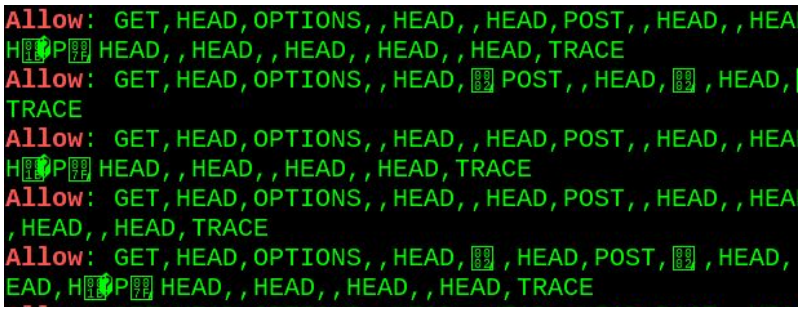

Figura 1: Cabeceras Allow que contienen datos de memoria

La vulnerabilidad puede ser explotada cuando se ha utilizado la directiva "Limit" con un método HTTP inválido, como por ejemplo en un .htaccess como este:

```
<Limit abcxyz>
</Limit>
```

El método podría ser considerado inválido tanto por un error de tipeo o también por incluir un método que ha sido desactivado en la configuración global.

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 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Si bien, esta situación no es frecuente, el riesgo es mayor en aquellos servidores en ambientes de hosting compartido, debido a que la corrupción no está limitada a un solo virtual host; cualquier usuario de un servicio de hosting compartido podría crear un .htaccess de forma deliberada para causar la corrupción en otros servidores.

Esta vulnerabilidad se ha bautizado OPTIONbleed debido a ciertas similitudes con la vulnerabilidad Heartbleed que afectó a OpenSSL que permitía leer porciones arbitrarias de la memoria mediante peticiones construidas especialmente. Sin embargo, debido a que la explotación de la misma depende de la combinación de la vulnerabilidad con una configuración poco usual, la criticidad de OPTIONbleed es menor. La criticidad aumenta en ambientes de hosting compartidos y/o en servidores que alojan aplicaciones web vulnerables que permitan la inyección y/o modificación de un archivo .htaccess.

Detección:

Para determinar si un servidor es vulnerable, se puede ejecutar el siguiente comando:

```
for i in {1..100}; do curl -sI -X OPTIONS http://www.midominio.com/|grep -i
"allow:"; done
```

El investigador que descubrió la vulnerabilidad ha publicado un script en python para verificar la vulnerabilidad:

https://github.com/hannob/optionsbleed

Se debe tener en cuenta que, por las características de la vulnerabilidad, no puede predecirse el comportamiento de forma sistemática, por lo que el script podría arrojar falsos negativos. Las pruebas deben realizarse en momentos en que el servidor tiene un alto nivel de uso. En algunas ocasiones, las respuestas corruptas aparecen recién después de múltiples peticiones.

Impacto:

Un cibercriminal podría obtener información sensible, tanto del propio servidor (contraseñas, por ejemplo), como de los usuarios que lo visitan.

Mitigación y Solución:

Las vulnerabilidades fueron corregidas mediante un parche de Apache HTTP. En el caso de sistemas operativos Linux, las actualizaciones han sido disponibilizado en la gran mayoría de las distribuciones.

- Debian
- Ubuntu

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 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

- Gentoo
- NetBSD/pkgsrc
- Guix
- Arch Linux
- Slackware
- NixOS

También se puede descargar el parche en el siguiente enlace:
https://svn.apache.org/viewvc/httpd/httpd/branches/2.4.x/server/core.c?r1=1805223&r2=1807754&pathrev=1807754&view=patch
Para Apache 2.2.x se puede descargar el siguiente parche:
https://blog.fuzzing-project.org/uploads/apache-2.2-optionsbleed-backport.patch

De modo a mitigar la vulnerabilidad, se puede eliminar y/o corregir todas las directivas Limit que contengan un método HTTP inválido o no registrado globalmente. Esta mitigación no es suficiente en servidores en ambientes de hosting compartido.

Información adicional:
https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html
https://mail-archives.apache.org/mod_mbox/httpd-dev//201709.mbox/%3CCACsi253RfX7OT5NhZCKRru2JpOKoscux%3DjzDzJOnbcF31XHmMw%40mail.gmail.com%3E
https://nvd.nist.gov/vuln/detail/CVE-2017-9798

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 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py