Departamento de Seguridad Informática MINSAP

Septiembre 2017

Volumen 1, nº 1

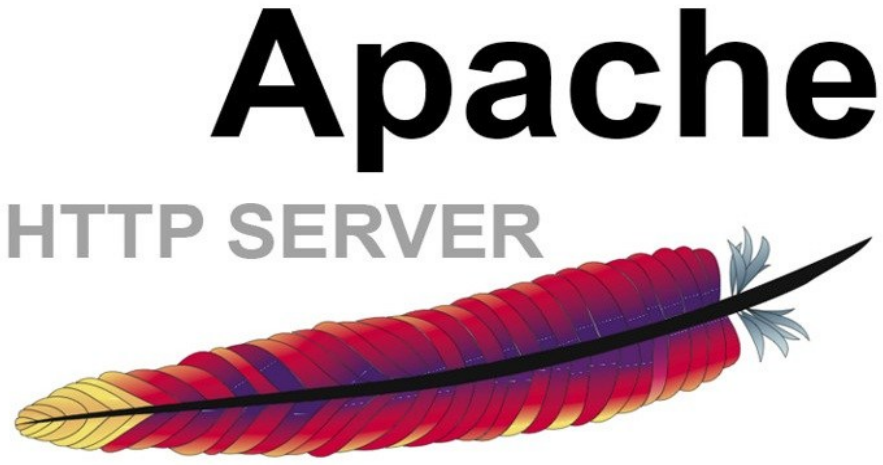
Boletín de Seguridad Informática

Contenido:

Puntos de interés especial:

- La vulnerabilidad tiene ciertas similitudes con el conocido y dramático Heartbleed
- **TP-Link**, la multinacional china dedicada a la fabricación de productos relacionados con la conectividad
- La conocida herramienta de limpieza para Windows **CCleaner** dio hace unos días uno de los sustos del año al conseguir un grupo de hackers introducir una puerta trasera que podía ser utilizada para instalar malware, keyloggers y ransomware.

Optionsbleed es una filtración de memoria que afecta al servidor HTTP Apache



El investigador en seguridad Hanno Böck ha detallado el último lunes un problema de seguridad al que ha decidido llamar **Optionsbleed**, debido a que **ciertas configuraciones en el servidor HTTP Apache pueden provocar una filtración de los datos alojados en la memoria**.

La vulnerabilidad tiene ciertas similitudes con el conocido y dramático Heartbleed, sobre todo en la manera en que los atacantes pueden realizar peticiones a los servidores para engañar al servidor Apache con el fin de obtener como respuesta más datos de los que les corresponde desde su posición.

Böck explica que Optionsbleed no es tan grave como Heartebleed porque **solo filtra contenidos procesados por el servidor** Apache y no contenidos de todo tipo alojados en la memoria de la máquina, incluyendo el sistema operativo y otros programas y aplicaciones. Esto significa que **la filtración de datos está limitada a lo que Apache procesa**, destacando las páginas web muy por encima del resto. Sin embargo, esto no significa que la vulnerabilidad sea inocua, ya que sí se podría filtrar contenidos de páginas reservadas solo a usuarios autenticados. Básicamente, los servidores HTTP se dedican a servir datos que tienen alojados según las peticiones realizadas por los clientes, que principalmente son navegadores web. Los clientes suelen realizar peticiones de tipo GET o POST y esperan obtener una respuesta de los servidores. Sin embargo, Apache es capaz de procesar otros tipos de peticiones a través de sus “métodos”, pudiéndose mencionar PUT, PATCH, HEAD, etc. Estos métodos han sido añadidos a Apache con el paso de los años y no están soportados por todos sus competidores

Además, los administradores de servidores también bloquean el acceso a algunos de esos métodos.

Con el fin de no convertir las peticiones a los servidores en un agujero negro, Apache es capaz de soportar los métodos a modo de opción. Un cliente puede consultar al servidor con una petición de opciones y el servidor responde qué métodos tiene permitidos.

En las opciones permitidas (Allow) se pueden **ver porciones aleatorias que parecen pertenecientes a páginas web**, lo que puede ser interpretado como una filtración de código. Böck no ha sido capaz de hallar el origen exacto del fallo, por lo que ha decidido reportar lo que tiene al equipo de seguridad de Apache.

Todo parece indicar que el origen está en ciertas configuraciones del servidor Apache que terminan provocando Optionsbleed, por lo que no estamos ante un problema generalizado ni especialmente extendido. De hecho, parece que el origen viene de una configuración errónea del fichero *.htaccess*:

```
< Limits PATCH PUT DELETE >
 Deny from all
< /Limits >
```

Los ficheros *.htaccess* pueden ser colocados dentro de las carpetas de un servidor Apache para establecerles normas concretas. Esto permite a los administradores de los servidores limitar las opciones que pueden ser solicitadas por los clientes. Sin embargo, parece que el **establecer normas contradictorias en un fichero *.htaccess* puede terminar confundiendo al servidor, provocando la vulnerabilidad Optionsbleed**, que puede ser etiquetada como de *usar después de liberar* memoria.

Optionsbleed no fue descubierto por Böck, sino que ha tomado como referencia un informe que lo describía en 2014 publicado por investigadores Old Dominion University, en Estados Unidos. Después de tres años, desde Apache solo han lanzado parches para las ramas 2.4.X y 2.2.X.

Los servidores Apache que están funcionando en entornos compartidos, en los cuales se pueden encontrar diferentes implementaciones del fichero *.htaccess* en una misma máquina, son los más afectados por Optionsbleed.

HomeCare es la solución de TP-Link para proteger la red inalámbrica del hogar

TP-Link, la multinacional china dedicada a la fabricación de productos relacionados con la conectividad, presentó el día de ayer **HomeCare** , su solución de conectividad y seguridad para el hogar disponible para algunos de sus productos, y que está reforzado con el software antimalware de **Trend Micro**.

HomeCare de TP-Link es una solución creada con el fin de ofrecer protección integrada para una red inalámbrica doméstica e impedir el acceso a esta por parte de cibercrminales, todo esto sin que la velocidad de conexión se vea afectada. De sus características se puede destacar un **control parental para gestionar la actividad online** y ofrece información adicional para garantizar la seguridad. El software de seguridad de Trend Micro se encarga de **proteger la red inalámbrica y los dispositivos conectados de posibles intrusiones**, además de bloquear sitios web maliciosos para impedir el acceso a estos por parte de los usuarios. Mientras, un escáner que está activo permanentemente se encarga de detectar patrones de malware para identificar y eliminar las amenazas contra la red del hogar.

El software de Trend Micro también cuenta con una capa adicional que pone en cuarentena cualquier dispositivo infectado que se conecte a la red, avisando de forma inmediata al usuario e indicándole los pasos a seguir para solucionar el problema. Por otro lado, este software de seguridad es actuali-

zado por la propia Trend Micro.

El **control parental permite crear perfiles por cada usuario**, permitiendo al administrador de HomeCare controlar los dispositivos que están siendo usados por los niños y aplicar filtros para impedir el acceso a contenidos inapropiados, además de poder ajustar el tiempo máximo de conexión. HomeCare permite **aplicar esta gestión a nivel del dispositivo**, sin necesidad de que se encuentre conectado a la red del hogar.

La característica de Calidad del Servicio (QoS en sus siglas en inglés) se encarga de que la red siempre ofrezca la misma velocidad de conexión y de ajustar el ancho de banda según las necesidades para priorizar los sitios web que más lo necesitan, permitiendo ofrecer una experiencia más fluida con Internet y poder, por ejemplo, jugar online sin que esto impacte al uso de Internet realizado desde otros dispositivos.

Las prestaciones de HomeCare ya están disponibles a través de una actualización de firmware para los dispositivos Deco M5, Archer C5400, Archer C3150 y Archer C2300.

Cada mes aparecen 1,4 millones de sitios web falsos que realizan phishing

Según informe publicado por Webroot, en lo que llevamos de año **se han creado cada mes 1,4 millones de sitios web falsos que realizan phishing**. Esto muestra que este método de ataque para robar datos ha sido efectivo con el paso del tiempo, ya que el número de sitio web falsos detectados es considerable.

El mes en el que se han registrado más sitios web de phishing fue **mayo, con un total de 2,3 millones**. El informe recalca la cada vez mayor sofisticación de los ataques de phishing, algo de lo que hemos informado en anteriores ocasiones en MuySeguridad. Los sitios web falsos son cada vez más difíciles de detectar, ya que los ciberdelincuentes han ido cubriendo cada vez más flecos en sus creaciones, siendo las falsificaciones cada vez más conseguidas y más difíciles de distinguir del contenido original y legal.

Sin embargo, un punto importante que recalca Webroot es la **fugacidad de los sitios web creados para realizar ataques de phishing, los cuales solo están activos entre cuatro y ocho horas** la mayoría de las veces. Este método de proceder es utilizado con el fin de evitar su rastreo y el acabar en listas negras, que obviamente permitirían a un navegador web bloquear la falsificación antes de que el usuario acceda.

Los sitios web más falsificados, como no podía ser de otra forma, son los más populares, pudiéndose mencionar a Google, Chase, Dropbox, PayPal y Facebook. Los engaños llegan a costar a las empresas estadounidenses unos 500 millones de dólares al año.

Para Webroot, la mejor forma de combatir el phishing por parte de la industria de la ciberseguridad sería adoptando *"una combinación de educación del usuario y protección organizacional con inteligencia en tiempo real para estar por delante del cambiante escenario de amenazas."*

Descubren esparcimiento de malware usando la puerta trasera de CCleaner

La conocida herramienta de limpieza para Windows **CCleaner** dio hace unos días uno de los sustos del año al conseguir un grupo de hackers introducir una puerta trasera que podía ser utilizada para instalar malware, keyloggers y ransomware. El hecho de que Windows suela funcionar con privilegios de administrador ayuda bastante a los actores maliciosos.

Tras ser reportado, los desarrolladores de CCleaner lanzaron de forma de rápida una versión parcheada de la aplicación y los investigadores que descubrieron las versiones troyanizadas descartaron un segundo escenario, sin embargo, esto último ha sido refutado hace poco, ya que investigadores de Talos Group, perteneciente a Cisco, han encontrado **evidencias de una carga útil hallada en el fichero *GeeSetup_x86.dll***, que fue enviado a listas específicas de computadoras basadas en nombres de dominios locales.

La lista predefinida fue hallada en el servidor de mando y control de los desarrolladores de la puerta trasera introducida en CCleaner, y estaba diseñada para encontrar computadoras conectadas a redes pertenecientes a grandes empresas de tecnología, las cuales serían el objetivo de esta carga útil. Las empresas objetivo eran las siguientes:

- Google
- Microsoft
- Cisco
- Intel
- Samsung
- Sony
- HTC
- Linksys
- D-Link
- Akamai

En la base de datos del servidor de mando y control se han encontrado a cerca de 700.000 ordenadores en las cuales se ha conseguido instalar la puerta trasera y **al menos 20 (unidades) que fueron infectadas con la carga útil**.

Las 20 computadoras infectadas con la carga útil fueron halladas utilizando nombre de dominio, dirección IP y nombre de host. Esto ha llevado a los investigadores de Talos Group a llegar

a la conclusión de que **podría tratarse de un malware creado para propósitos de espionaje industrial**.

Un grupo de hackers chino podría estar detrás del ataque

La compañía de ciberseguridad Kaspersky Lab ha señalado que el autor de la puerta trasera y la carga útil sería un experto grupo de hackers chino llamado Axiom, que también habría actuado bajo nombres como APT17, Group 72, DeputyDog, Tailgater Team, Hidden Lynx y AuroraPanda. Esa es la conclusión a la que ha llegado tras encontrar en el malware distribuido mediante CCleaner código utilizado por el mencionado grupo.

Los investigadores de Cisco han encontrado un fichero de configuración en el servidor de los atacantes que establecía un horario perteneciente a una zona de China. Aunque esto no resulta en sí mismo concluyente para determinar que Axiom estuviera detrás de toda esta operación maliciosa, podría ser interpretado como una evidencia. Por otro lado, han notificado a las compañías afectadas nada más realizar su descubrimiento.

La carga útil no se elimina actualizando CCleaner

La puerta trasera podía ser eliminada mediante la actualización de la aplicación, pero no se puede decir lo mismo la carga útil, la cual **solo puede ser eliminada mediante el uso de un antimalware o bien restaurando imágenes previas del sistema** pertenecientes a un algún momento anterior a la instalación de la carga útil.

Un popular antivirus chino para Android ha estado recolectando datos de forma ilegítima

Un popular antivirus chino presente en la Play Store para Android, **DU Antivirus Security**, ha sido eliminado y restituido por Google tras detectar Check Point que estaba realizando una **recolección de datos ilegítima**.

Según los datos que se pueden extraer de la propia Play Store, DU Antivirus Security ha sido descargado entre 10 y 50 millones de veces, por lo que estamos hablando de una aplicación que ha conseguido cierta notoriedad en su segmento. Sin embargo, los investigadores de Check Point descubrieron que, además de presuntamente proteger los dispositivos Android del malware, ha estado **recolectando datos como identificadores únicos, lista de contactos, registros de llamadas e información de localización**.

En el proceso de recolección de datos DU Antivirus Security **los cifraba y los enviaba a un servidor** cuya IP era 47.88.174.218. Al principio los investigadores pensaron que pertenecía al autor de algún malware, pero tras investigar descubrieron que los registros de DNS y los subdominios adyacentes mostraban que los dominios principales estaban almacenados en un **servidor registrado por un empleado de Baidu** (el "Google chino") llamado Zhan Liang Liu.

Los datos recolectados eran luego usados en otra aplicación llamada "Caller ID & Call Block – DU Caller", la cual también pertenece a DU Group y ofrece información a los usuarios sobre las llamadas de entrada.

Tras ser notificada de forma secreta por Check Point, Google decidió eliminar DU Antivirus Security el 21 de agosto, aunque **permitió que volviera el 24 del mismo mes después de que su desarrollador eliminase el código encargado de recolectar la información de los usuarios**. Como defensa de su acción, Google ha argumentado que aquel mecanismo no estaba especificado en la política de privacidad ni en la obtención de permisos del usuario en el proceso de instalación. Las versiones afectadas de la aplicación son la v3.1.5 y posiblemente las anteriores, según Check Point.

Sin embargo, el mecanismo de recolección ilegítima hallado en DU Antivirus Security no termina ahí, ya que este ha sido encontrado en otras 30 aplicaciones, de las cuales 12 están o estaban presentes en la Play Store. Según la estadísticas de la tienda de Google, han sido descargadas entre 24 y 89 millones de veces, lo que delata el gran impacto de este software, que puede ser etiquetado como malware.

Check Point ha publicado una lista de las aplicaciones encontradas en la Play Store que utilizan el mecanismo de recolección de datos ilegítimo junto a las que está fuera de la tienda.

Aplicaciones halladas fuera de la Play Store:

- com.power.core.setting
- com.friendivity.biohazard.mobo
- com.energyprotector.tool
- com.power.core.message
- batterysaver.cleaner.speedbooster.taskkiller.phonecooler
- com.rammanager.pro
- com.memoryanalysis.speedbooster
- com.whosthat.callerid
- speedbooster.memorycleaner.phonecleaner.phonecooler
- com.example.demos
- com.android.fb
- antivirus.mobilesecurity.antivirusfree.antivirusandroid
- speedtest.networksecurity.internetbooster
- com.ramreleaser.speedbooster
- com.dianxinos.optimizer.duplay
- com.coolkeeper.instacooler
- com.memoryreleaser.booster