Salto de certificados en Apache con HTTP/2

Se ha anunciado una vulnerabilidad en el servidor web Apache HTTPD (versiones 2.4.18-2.4.20) por la que se salta la validación de certificados cliente X509 cuando se hace uso del módulo experimental HTTP/2.

Apache es el servidor web más popular del mundo, usado por más del 52% de los sitios web, disponible en código fuente y para infinidad de plataformas, incluyendo diversas implementaciones de UNIX, Microsoft Windows, OS/2 y Novell NetWare.

En la versión 2.4.17 de Apache HTTP Server se introdujo como función experimental el módulo mod_http2 para el soporte del protocolo HTTP/2. El problema, con **CVE-2016-4979**, reside en que el servidor web Apache HTTPD no valida los certificados de cliente X509 correctamente cuando se utiliza este módulo para acceder a un recurso. El resultado es que se puede acceder a un recurso que requiere un certificado de cliente válido sin dicha credencial.

Hay que señalar que el impacto es muy limitado, ya que este módulo está compilado y no se activa por defecto (aunque alguna distribución sí pueda hacerlo). Generalmente necesita activarse en la línea de Protocols del archivo de configuración de Apache agregando "h2" y/o "h2c" al "http/1.1".

Por ende, se ha publicado la versión 2.4.23 del servidor web Apache que soluciona esta vulnerabilidad, disponible desde:
http://httpd.apache.org/download.cgi

Más información:

- CVE-2016-4979: HTTPD webserver - X509 Client certificate based authentication can be bypassed when HTTP/2 is used [vs]
  https://mail-archives.apache.org/mod_mbox/httpd-announce/201607.mbox/CVE-2016-4979-68283

- Apache HTTP Server 2.4.23 Released
  https://www.apache.org/dist/httpd/Announcement2.4.html

- Apache httpd 2.4 vulnerabilities
  http://httpd.apache.org/security/vulnerabilities_24.html

Fuente: Hispasec

Cross-Site Request Forgery en Fortinet Web

Fortinet ha publicado un boletín de seguridad para alertar de una vulnerabilidad de cross-site request forgery (CSRF) en dispositivos FortiWeb.

La técnica llamada falsificación de petición en sitios cruzados (CSRF) consiste en un ataque fuerza al navegador web de la víctima, validado en algún servicio (como por ejemplo correo o home banking) a enviar una petición a una aplicación web vulnerable, esta aplicación se encarga de realizar la acción elegida a través de la víctima, debido que la actividad maliciosa será procesada en nombre del usuario logueado.

Fortinet FortiWeb 400C

La familia FortiWeb de firewall para aplicaciones web de Fortinet ofrece seguridad tanto para aplicaciones web como XML en una sola plataforma. Los dispositivos FortiWeb están diseñados para brindar protección frente ataques (como inyección SQL o XSS) al nivel de aplicación.

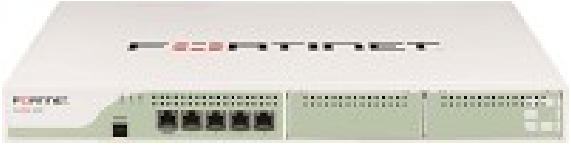
El problema, con **CVE-2016-4066**, reside en un error de validación de las entradas del usuario que podría permitir a un atacante remoto realizar ataques de cross-site request forgery. Este tipo de vulnerabilidades permiten a un atacante ejecutar funcionalidades de una web determinada a través de la sesión de otro usuario en esa web. De esta forma un atacante podría tener acceso al servidor con los mismos permisos que los del usuario atacado. Por ejemplo, mediante el uso de un formulario específicamente diseñado el atacante podría llegar a cambiar la contraseña administrativa.

Fortinet ha publicado la versión de software FortWeb 5.5.3 que corrige la vulnerabilidad.

Más información:

FortiWeb CSRF Vulnerability
http://fortiguard.com/advisory/fortiweb-csrf-vulnerability

FortiWeb: cortafuegos para aplicaciones web
http://www.fortinet.es/productos/proteccion-de-aplicaciones/aplicaciones-web.html



Fuente: Hispasec

HTTPoxy: vulnerabilidad en Apache/Ngnix/PHP/Go/Python redescubierta después de 15 años

Peligrosas vulnerabilidades descubiertas hace 15 años han aparecido nuevamente dejando potencialmente abierto cualquier servidor web. La vulnerabilidad fue bautizada como HTTPoxy y está ligada a un error encontrado por Randal Schwartzen en Perl en el 2001. En el mismo año también fue identificada en curl, en 2012 en Ruby y en 2013 en Nginx.

Esta vez se ha encontrado en los lenguajes PHP, Python y Go. La Fundación de Software Apache, Red Hat, Ngnix y otros se han apresurado a informar sobre HTTPoxy que es un compendio de las siguientes vulnerabilidades en implementaciones CGI:
CVE-2016-5385: PHP
CVE-2016-5386: Go
CVE-2016-5387: Apache HTTP Server
CVE-2016-5388: Apache Tomcat
CVE-2016-1000109: HHVM
CVE-2016-1000110: Python

Este agujero de seguridad en bibliotecas populares pueden explotarse para buscar información en sitios vulnerables y potencialmente se podría acceder a datos sensibles y tomar el control del código fuente y del servidor. HTTPoxy se puede explotar a través de aplicaciones basadas en CGI, como en el caso del CVE-2012-1823 que tantos problemas generó.

Básicamente, es un abuso de la cabecera HTTP_PROXY en una solicitud al servidor web. Debido a un conflicto de nombres, la aplicación web podría utiliza el servidor proxy definido por esa variable para cualquier tipo de conexión HTTP saliente. La convención de nomenclaturas para los campos de encabezado HTTP en las variables de entorno CGI definidas por la RFC 3875 son convertidas a mayúsculas y tienen el prefijo "HTTP_".

Si un cliente envía un cabecera "Proxy" algunas implementaciones de CGI crearán una variable de entorno "HTTP_PROXY" que anula la variable real del mismo nombre. Por lo tanto, si el HTTP_PROXY es un servidor malintencionado (Ej: Proxy: evil.example.com), este puede interceptar las conexiones de la aplicación web a otros sistemas y, dependiendo de cómo está diseñado el código, potencialmente obtener una ejecución remota de código.

Hay avisos disponibles ahora de Apache, Red Hat, US CERT, Nginx, y Drupal y aquí se puede conseguir una guía no técnica. Microsoft IIS también puede ser afectado si se ejecutan aplicaciones CGI o de terceros. Si se desean detalles técnicos se pueden analizar las pruebas de concepto publicadas en Github.

Para llevar a cabo la mitigación se debe bloquear el uso de la cabecera Proxy en el servidor web.
Parchea inmediatamente

Fuente: segu-info

Actualizaciones de Drupal, Joomla y Wordpress

Drupal 8.1.7 y 7.50

El equipo de Drupal acaba de publicar una nueva actualización para la rama 8.1.7 que corrige una vulnerabilidad de seguridad catalogada como muy crítica (SA-CORE-2016-003). Además la versión también está considerada como de mantenimiento con cambios para el .htaccess y web.config (ver notas de la versión).

Además, Drupal acaba de publicar una actualización para la rama 7 considerada de mantenimiento y que por lo tanto no incluye ninguna corrección de seguridad. Esta actualización corrige errores de las versiones anteriores, nuevas características y mejoras.

Joomla! 3.6.0

El equipo de Joomla! acaba de anunciar el lanzamiento de Joomla! 3.6. Esta nueva versión incorpora unas 400 mejoras de todo tipo, haciendo especial hincapié en la mejora de experiencia de usuario (UX).

Se puede actualizar únicamente el núcleo, pudiendo sobreescribir cualquier archivo modificado y del mismo revertirlos al estado predeterminado.

WordPress 4.5.3

Se ha publicado una actualización de seguridad de WordPress 4.5.3, que según el sitio oficial en Español, solventa las varias vulnerabilidades importantes de XSS.

Se recomienda actualizar a la mayor brevedad posible. Info en el trac de WordPress y lista de cambios.