Actualización de Seguridad de Subversión

Apache ha publicado Subversion 1.8.16 y 1.9.4 destinadas a solucionar dos vulnerabilidades que podrían permitir provocar denegaciones de servicio o la posibilidad de autenticación con "realms" erróneos.

Subversion es un sistema de control de versiones Open Source, que en la actualidad pertenece a la Apache Software Foundation. Utiliza el concepto de revisión para guardar los cambios producidos en el repositorio, además de proporcionar un entorno eficiente y muy flexible.

El primer problema, con **CVE-2016-2167**, reside en que svnserve (el protocol de servidor svn://) puede utilizar de forma opcional la librería Cyrus SASL para autenticación, integridad y cifrado. Debido a un error de programación, la autenticación contra Cyrus SASL podría permitir a un usuario remoto especificar una cadena realm que sea el prefijo de la cadena realm esperada. Esto podría permitir la autenticación en otros realms diferentes. Por ejemplo, el usuario "prueba" en el realm "Texto", podría autenticarse con éxito en un repositorio cuyo realm sea "TextoNuevo". Solo afecta a repositorios servidor por svnserve usando SASL.

Por otra parte, con **CVE-2016-2168**, una vulnerabilidad de denegación de servicio en servidores httpd de Subversion en el módulo mod_authz_svn. El fallo se produce durante la comprobación de la autorización de peticiones COPY o MOVE con cabeceras específicamente manipuladas.

Apache ha publicado las versiones 1.8.16 y 1.9.4 que solucionan estos problemas, y otros fallos no relacionados con problemas de seguridad. Se encuentran disponibles desde:

- http://subversion.apache.org/packages.html

Más Información:

svnserve/sasl may authenticate users using the wrong realm

- http://subversion.apache.org/security/CVE-2016-2167-advisory.txt

Remotely triggerable DoS vulnerability in mod_authz_svn during COPY/MOVE authorization check.

- http://subversion.apache.org/security/CVE-2016-2168-advisory.txt

Backdoor encontrado en Linux 3.4-sunxi afecta procesadores ARM

Un dispositivo Android puede ser sencillo de vulnerar si se tiene la suerte de encontrar una puerta trasera en el procesador. Gracias a Allwinner, un fabricante chino de chip, recientemente se ha descubierto una versión del Kernel de Linux que permite rootear el teléfono de forma muy simple y fácil, a través de una puerta trasera integrada.

La compañía de semiconductores China Allwinner es un proveedor de procesadores ARM que se utilizan en muchas tabletas Android de bajo costo y otros dispositivos electrónicos en todo el mundo. El agujero de seguridad está en cada imagen del sistema operativo para dispositivos A83T, H3 o H8 que dependen del Kernel Linux 3.4-sunxi. Este Kernel fue desarrollado para los procesadores de Allwinner y luego se adaptó para otros procesadores como Banana Pi micro-PCs y Orange Pi.

Todo lo que necesita para obtener acceso a la raíz de un dispositivo Android afectado es enviar el texto "rootmydevice" a cualquier proceso depuración. El código del backdoor permite escalamiento de privilegios locales de depuración del dispositivo y se cree que el código de la puerta trasera se ha quedado por error después de completar el proceso de depuración.

Aprovechando este error cualquier proceso que se ejecuta con cualquier UID se puede convertir en root fácilmente, simplemente usando el siguiente comando:

echo "rootmydevice" > /proc/sunxi_debug/sunxi_debug

En el foro del sistema operativo de Armbian, un moderador señaló que "el código de la puerta trasera podría ser explotable remotamente si se combina con servicios de red que permitan el acceso a /proc."

```
tk@bananapim3:~$ id
uid=1000(tk) gid=1000(tk) groups=1000(tk),20(dialout),27(sudo),29(audio),44(video),46(plugdev
tk@bananapim3:~$ echo "rootmydevice" > /proc/sunxi_debug/sunxi_debug
tk@bananapim3:~$ id
uid=0(root) gid=0(root) groups=0(root),20(dialout),27(sudo),29(audio),44(video),46(plugdev),1
```

David Manouchehri dió a conocer la información sobre la puerta trasera a través de su cuenta de Github y aparentemente fue eliminado y por eso se publicó en el siguiente URL: http://pastebin.com/sjej62iz

Fuente: The Hacker News

Denegaciones de Servicio en Cisco Web Security Appliance

Cisco ha anunciado la existencia de cuatro vulnerabilidades en los dispositivos Cisco Web Security Appliance (WSA) que podrían permitir a un atacante provocar condiciones de denegación de servicio.

Los dispositivos de seguridad Cisco Web Security Appliance (WSA) combinan defensa contra amenazas avanzadas, protección frente a malware avanzado, control y visibilidad de aplicaciones, informes detallados y movilidad segura en una única solución; además también permiten proteger y controlar el tráfico web. Estos dispositivos ejecutan el sistema operativo Cisco AsyncOS.

El primer problema, con CVE-2016-1380, reside en el tratamiento de peticiones HTTP POST con Cisco AsyncOS para Cisco Web Security Appliance (WSA) debido a que el proceso proxy deje de responder. Por otra parte, con CVE-2016-1381, un fallo en la liberación de memoria en las peticiones de un rango de archivos en caché de Cisco AsyncOS paraWSA podría llevar al dispositivo a quedarse sin memoria del sistema.

Con CVE-2016-1382, una vulnerabilidad en el tratamiento de peticiones HTTP debido a una asignación inadecuada del espacio para la cabecera HTTP y cualquier contenido HTTP esperado. Por último, con CVE-2016-1383, una vulnerabilidad en Cisco AsyncOS para Cisco Web Security Appliance (WSA) cuando trata un código de respuesta http específico podría dejar al dispositivo sin memoria del sistema.

Cisco ha publicado la versión 9.0.1-162 destinada a solucionar los problemas descritos. En la mayoría de los casos un WSA puede actualizarse desde Internet mediante la opción "System Upgrade" en la interfaz de administración del sistema. (System Administration/ System Upgrade/Upgrade Options/Download and Install).

Más información:

Cisco Web Security Appliance HTTP POST Denial of Service Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa1

Cisco Web Security Appliance Cached Range Request Denial of Service Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa2

Cisco Web Security Appliance HTTP Length Denial of Service Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa3

Cisco Web Security Appliance Connection Denial of Service Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160518-wsa4

Cisco Web Security Appliance
http://www.cisco.com/web/ES/products/security/web-security-appliance/index.html

Actualizaciones de seguridad de PHP. Moodle y WordPress

El equipo de desarrollo de **PHP** ha publicado actualizaciones para las ramas 7.0, 5.6 y 5.5 de PHP para solucionar múltiples vulnerabilidades que pueden ser aprovechadas para provocar denegaciones de servicio e incluso comprometer los sistemas afectados.

Además, las nuevas versiones publicadas también incluyen la corrección de otros problemas no relacionados directamente con la seguridad.

De igual manera, se han liberado nuevas versiones para diferentes ramas de **Moodle**, el CMS Open Source posiblemente más usado de la formación online.

En concreto son las versiones: Moodle 3.0.4, 2.9.6, 2.8.12 y 2.7.14 y están disponibles desde el canal de descargas habitual https://download.moodle.org o vía Git.

Además de varios bugs relativos a su funcionamiento, se han parcheado varios fallos de seguridad por lo que desde Moodle se recomienda actualizar con brevedad las instalaciones afectadas.

Moodle 3.0.4 release notes
Moodle 2.9.6 release notes
Moodle 2.8.12 release notes
Moodle 2.7.14 release notes

Asimismo, se ha publicado una actualización de seguridad de **WordPress** etiquetada bajo el número de versión 4.5.2, que según su el sitio oficial en Español, solventa las siguientes vulnerabilidades:

Las versiones de WordPress 4.5.1 y anteriores están afectadas por ALGUNA vulnerabilidad debida a Plupload, la biblioteca externa que usa WordPress para subir archivos. Las versiones de WordPress desde la 4.2 hsta la 4.5.1 son vulnerables a un ataque de XSS reflejo si se utilizan URLs especialmente creadas desde MediaElement.js, la biblioteca externa utilizada para los reproductores de medios. MediaElement.js y Plupload también se han actualizado para solucionar estos problemas.

Además de esto, existen varias vulnerabilidades ampliamente publicadas en la biblioteca de procesamiento de imágenes **ImageMagick**, utilizadas por los alojamientos web y compatibles con WordPress.
Ver: http://www.vencert.gob.ve/es-ve/news/2016/05/15/vulnerabilidades-criticas-en-imagemagick-exponen-millones-de-sitios-web/