BOLETÍN DE ALERTA

Boletín Nro.: 2016-03
Fecha de publicación: 15/01/2016
Tema: Vulnerabilidades críticas en cliente OpenSSH

Sistemas afectados:

- Las versiones de clientes OpenSSH 5.4 a 7.1p1
- OpenSSH se encuentra incluido en numerosos productos, algunos de los cuales incluyen el código vulnerable: https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=456088&SearchOrder=4

Descripción:

Los clientes OpenSSH de las versiones afectadas contienen el código necesario para el soporte experimental de la reanudación de las conexiones SSH (itinerancia). Si la conexión a un servidor SSH se corta inesperadamente, y si el servidor soporta la itinerancia, así, el cliente es capaz de volver a conectar con el servidor y reanudar la sesión SSH suspendida.

Dicha funcionalidad todavía no ha sido incluida en el código del servidor, sin embargo el código del cliente se encuentra activado por defecto y presenta dos vulnerabilidades críticas: una vulnerabilidad de fuga de información (CVE-2016-0777) y otra de *buffer overflow* (CVE-2016-0778).

La primera de ellas, CVE-2016-0777 puede ser explotada para que un servidor malicioso engañe al cliente vulnerable para que éste devuelva información de la memoria del cliente, incluyendo las claves privadas del usuario cliente.

La autenticación de las claves del servidor impide la explotación mediante un ataque *man-in-the-middle* (hombre-en-el-medio), por lo que esta fuga de información está restringida únicamente a las conexiones a los servidores maliciosos o comprometidos.

La vulnerabilidad de buffer overflow afecta a las funciones packet_write_wait y ssh_packet_write_wait(), las cuales pueden desbordarse en algunos escenarios después de una reconexión exitosa.

Si bien, la vulnerabilidad se encuentra presente en la configuración por defecto del cliente OpenSSH, su explotación requiere dos configuraciones no predeterminadas: un ProxyCommand, y, ForwardAgent (-A) o ForwardX11 (-X). Por lo tanto, es poco probable que este desbordamiento de

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

búfer tenga un impacto en el mundo real, sin embargo, puede ser explotado en sistemas que utilizan configuraciones personalizadas.

Las vulnerabilidades fueron reportadas por el equipo de seguridad de Qualys. Puede encontrar los detalles en el siguiente enlace:

https://www.qualys.com/2016/01/14/cve-2016-0777-cve-2016-0778/openssh-cve-2016-0777-cve-2016-0778.txt

Impacto

Un usuario que se autentica a un servidor malicioso o comprometido puede revelar datos privados, incluyendo la clave privada del usuario, o causar un desbordamiento de búfer que puede provocar la ejecución remota de código en ciertas configuraciones no predeterminadas.

Mitigación y solución

El código vulnerable en el cliente puede ser completamente desactivado añadiendo 'UseRoaming no' en el archivo de configuración global de ssh, o en la configuración del usuario en ~ / .ssh / config, o mediante el comando -oUseRoaming=no en la línea de comandos.

Además, OpenSSH ha publicado una actualización que corrige las vulnerabilidades, la versión OpenSSH 7.1p2. Se recomienda actualizarlo cuanto antes. El procedimiento para la actualización varía de acuerdo al sistema afectado.

Información adicional:

http://www.openssh.com/txt/release-7.1p2

https://www.kb.cert.org/vuls/id/456088

https://www.qualys.com/2016/01/14/cve-2016-0777-cve-2016-0778/openssh-cve-2016-0777-cve-2016-0778.txt

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