avet
Information and Network Security

Krytyczna podatność w OpenSSH

AVET INS Security Monitoring Services

Odkryte krytyczne podatności w kliencie OpenSSH (CVE-2016-0777, CVE-2016-0778)

Wprowadzenie:

Wersje oprogramowania klienckiego OpenSSH w wersjach od 5.4 do 7.1 podatne są na atak umożliwiający wyciek pamięci oraz kradzież kluczy prywatnych. W przypadku, gdy połączenie SSH zostanie przerwane (np. poprzez błąd sieci) klient OpenSSH jest w stanie ponownie połączyć się z serwerem i za pomocą funkcjonalności „roaming" wznowić przerwaną sesję terminalową. Kod tej funkcjonalności po stronie klienta jest podatny m.in. na podatności typu buffer overflow oraz podatności wycieku pamięci.

Podatność ta możliwa jest do wykorzystania w przypadku, gdy klient połączy się z serwerem SSH posiadającym złośliwą funkcjonalność.

- CVE-2016-0777: *funkcja resend_bytes w pliku roaming_common.c w kliencie OpenSSH (w wersjach 5.x, 6.x oraz 7.x aż do wersji 7.1p2) pozwala zdalnym hostom na ujawnienie poufnych danych z pamięci procesu – w tym kluczy prywatnych.*

- CVE-2016-0778: *funkcje roaming_read oraz roaming_write w pliku roaming_common.c w kliencie OpenSSH (w wersjach 5.x, 6.x oraz 7.x aż do wersji 7.1p2) w niektórych przypadkach niepoprawnie*

zarządzają deskryptorami połączeń co może skutkować atakiem typu Denial of Service (przepełnienie sterty w pamięci) lub nieprzewidzianymi skutkami w procesie.

Należy zwrócić uwagę, iż tego typu podatność w systemach informatycznych firmy może skutkować wystąpieniem niezgodności w obszarze rekomendacji D KNF oraz PCI-DSS.

Rozwiązanie problemu:

Jeśli niemożliwa jest instalacja poprawki lub aktualizacja klienta OpenSSH (np. poprzez kompilację ze źrodeł) w celu zabezpieczenia się przed tą podatnością należy zaktualizować oprogramowanie klienckie OpenSSH do najnowszej wersji lub ręcznie wyłączyć opcję roaming w pliku /etc/ssh/ssh_config, dodając linię:

```
UseRoaming no
```

Można także wymusić wyłączenie opcji roamingu z linii poleceń klienta OpenSSH:

ssh -o 'UseRoaming no' [nazwa/adres hosta]

Należy podkreślić, iż opisane podatności dotyczą tylko klienta OpenSSH i nie dotyczy serwerów OpenSSH ani innych implementacji klientów SSH pod warunkiem, że nie bazują na źródłach OpenSSH. Wszystkie wersje klienta OpenSSH, które nie wspierają roamingu, także sa odporne na atak.

W systemach Linux w celu aktualizacji – zakładając dostępność poprawek – bazujących na dystrybucji Debian należy wydać polecenia:

sudo apt-get update && sudo apt-get upgrade

W systemach **RedHat i Fedora** należy wydać polecenie:

sudo yum update

Dodatkowe informacje dla systemów Red Hat: https://rhn.redhat.com/errata/RHSA-2016-0043.html
Dodatkowe informacje o instalacji poprawek w systemach Red Hat: https://access.redhat.com/articles/11258

Jeśli dla danego systemu nie ma dostępnych poprawek lub instalacja poprawek jest niemożliwa z jakiegoś powodu, nadal pozostaje możliwość aktualizacji klienta OpenSSH poprzez kompilację ze źródeł.

OpenBSD 5.8

Należy zainstalować poprawkę : 010: SECURITY FIX: January 14, 2016 dostępną pod adresem http://ftp.openbsd.org/pub/OpenBSD/patches/5.8/common/010_ssh.patch.sig

Poprawka jest dostępna dla wszystkich wspieranych przez OpenBSD architektur.

Aby zainstalować poprawkę należy zaaplikować patch i zrekompilować OpenSSH wydając polecenia:

```
signify -Vep /etc/signify/openbsd-58-base.pub -x 010_ssh.patch.sig \
    -m - | (cd /usr/src && patch -p0)
cd /usr/src/usr.bin/ssh
make obj && make depend && make && make install
```

Należy zauważyć, że aplikacja patcha wymaga rozpakowanych źródeł do katalogu /usr/src. Źrodła są dostępna na płycie CD z wydaniem OpenBSD lub na serwerach FTP/HTTP z kopią wydania 5.8 OpenBSD.

OpenBSD 5.8-current i OpenBSD 5.9

OpenBSD 5.8-current w dniu 20 stycznia 2016 nie był podatny na atak – aktualna wersja OpenSSH została podniesiona.

OpenBSD 5.9 nie jest podany na atak (analiza na podstawie źródeł OpenBSD 5.8-current)

Kompilacja ze źródeł wersji OpenSSH portable

Wersja OpenSSH-7.1p2 (http://www.openssh.com/txt/release-7.1p2) jest odporna na opisany atak. Wersja portbale jest przeznaczona dla innych systemów niż OpenBSD. Źródła wersji portable są do pobrania z jednego z mirrorów z listy dostępnej tutaj: http://www.openssh.com/portable.html

Nie zalecamy kompilacji ze źródeł z repozytorium git: anongit.mindrot.org/openssh.git ponieważ brakuje pliku makefile.

Przed kompilacją OpenSSH zalecana jest instalacja biblioteki LibreSSL, z której OpenSSH może korzystać w zastępstwie OpenSSL. Autorzy OpenSSH uważają bibliotekę LibreSSL za bezpieczniejszą implementację OpenSSL (uwaga: ABI nie jest zgodne pomiędzy bibliotekami).

Jeśli chcemy skompilować OpenSSH z LibreSSL a biblioteka nie jest zainstalowana w systemie, należy pobrać pliki:

wget http://ftp.openbsd.org/pub/OpenBSD/LibreSSL/libressl-2.2.5.tar.gz.asc

wget http://ftp.openbsd.org/pub/OpenBSD/LibreSSL/libressl-2.2.5.tar.gz

Następnie pobrać klucz PGP:

gpg --recv-key 4B708F96

Zweryfikować bibliotekę:

gpg --verify libressl-2.2.5.tar.gz.asc

Rozpakować bibliotekę:

tar zxvf ./libressl-2.2.5.tar.gz

Następnie skompilować bibliotekę:

cd ./libressl-2.2.5

./configure && make check

make install

Kompilacja OpenSSH przebiega podobnie – należy pobrać źródła z jednego z dostępnych mirrorów:

gpg --verify openssh-7.1p2.tar.gz.asc

tar zxvf ./ openssh-7.1p2.tar.gz

cd / openssh-7.1p2

./configure && make && make install