Debian での OpenSSH の TCP wrappers サポート

Kazuhiro NISHIYAMA

2017/06/18

OpenSSH 6.7 で削除

- **upstream で削除された**

http://www.openssh.com/txt/release-6.7 に

- sshd(8): Support for tcpwrappers/libwrap has been removed.

とある

とりあえず拒否

/etc/hosts.deny:

```
ALL: ALL
```

- TCP wrappers 対応は OpenSSH だけじゃない
- デフォルトは安全側に倒して拒否したい

すると……

- 繋がらなくなった
- 影響がないはずと思っていた openssh-server に影響がでた?

試しに許可

/etc/hosts.allow:

```
sshd: 127.0.0.1 [::1]
sshd: 10.
sshd: .jp
```

- localhost を許可
- 例として 10.0.0.0/8 を許可
- 今は関係ないけど、逆引きが .jp も許可

すると……

- 繋がった
- 何かがおかしい
- /usr/share/doc/openssh-server/changelog.Debian.gz をみてみることに

openssh (1:6.7p1-1) unstable; urgency=medium

1:6.7p1-1 の項目の一部を引用:

```
  * Restore TCP wrappers support, removed upstream in 6.7.  It is true that
    dropping this reduces preauth attack surface in sshd.  On the other
    hand, this support seems to be quite widely used, and abruptly dropping
    it (from the perspective of users who don't read openssh-unix-dev) could
    easily cause more serious problems in practice.  It's not entirely clear
    what the right long-term answer for Debian is, but it at least probably
    doesn't involve dropping this feature shortly before a freeze.
```

- いきなり消すと影響が大きいので、
  とりあえず戻した、という感じ?

いったんまとめ

- とりあえず stretch では、まだ TCP wrappers が使える
- この先どうなるかはわからない
- 鍵のロールオーバー https://www.debian.org/security/key-rollover/index.ja.html のようなこともあったので、個人的には Debian 独自が続くのは不安がある
- upstream との差が開かない方が望ましいので、そのうち外れるのでは、という気がする

確認環境

- Debian GNU/Linux 9.0 (stretch)
- openssh-server 1:7.4p1-10
- Ubuntu 16.04.2 LTS (xenial)
- openssh-server 1:7.2p2-4ubuntu2.2

ちなみに前のバージョンは?

- Debian GNU/Linux 8.8 (jessie)
- openssh-server 1:6.7p1-5+deb8u3
- Ubuntu 14.04.5 LTS (trusty)
- openssh-server 1:6.6p1-2ubuntu2.8

Restore は 1:6.7p1-1、つまり jessie の時点での話だった

jessie, stretch と残ったので、しばらく残るのか、突然消えるのか、まだわからなさそう