목차

TCP Wrapper 3
제외 된 이유 3
참조링크 4

TCP Wrapper

RHEL/CentOS 8 버전부터는 /etc/hosts.allow 나 /etc/hosts.deny 파일이 확인 되지 않으며 파일을 생성 후 기존 과 같이 허용이나 차단에 대한 룰을 입력 하여도 적용이 되지 않습니다

/etc/hosts.deny 에서의 적용 예시

```
ALL: 123.123.123.123
```

레드햇 문서에 따르면 tcp_wrappers 패키지가 RHEL8 에서 포함되어 있지 않으며 tcp_wrappers 의 기능을 firewalld 로 대체 하였다고 합니다.

- https://fedoraproject.org/wiki/Changes/Deprecate_TCP_wrappers

tcp_wrappers 패키지 자체는 EPEL 레파지토리에서 설치는 할수 있으나 sshd에서 libwrap.so.0 라이브러리 참조하고 있지 않기 때문에 사용이 불가하며 7버전과 8버전에서의 차이는 아래와 같이 확인 해볼 수 있습니다.

```
RHEL/CentOS8
[root]# ldd /usr/sbin/sshd | grep wrap
(결과 없음)

RHEL/CentOS7
[root]# ldd /usr/sbin/sshd | grep wrap
libwrap.so.0 => /lib64/libwrap.so.0 (0x00007f957f04a000)
```

즉, 8 버전부터는 sshd 패키지에 libwrap 라이브러리 참조를 제거 한 것이라고 볼 수 있으며 그래서 8 버전 부터는 /etc/hosts.deny 등을 통해 차단이 아닌 OS 방화벽인 firewalls 를 통해 차단을 수행 해야 합니다.

제외 된 이유

보통은 Fedora Linux 에서 부터 변경에 대한 정책이 결정이 되고 적용이 되게 됩니다. 그리고 이후 RHEL 이 적용(DownStream) 을 하게 되게 됩니다. 그래서 이러한 변경에 대한 내용은 Fedora Linux 의 문서에서 많이 확인이 가능 합니다.

https://fedoraproject.org/wiki/Changes/Deprecate_TCP_wrappers 에 내용이 잘 정리되어 있으며 사유로는 아래와 같은 내용이 기술되어 있습니다.

tcp_wrappers 마지막 버전은 20 년 전에 출시되었습니다(IPv6 지원은 나중에 추가되었지만) 당시에는 “ 모든 트래픽을 차단 ” 하는 매우 강력한 도구 였지만, 요즘에는 네트워크 수준의 모든 트래픽에 대해 firewalls/iptables/nftables 를 사용하여 동일한 작업을 수행하거나 애플리케이션 수준에서 유사한 필터링을 사용할 수 있습니다.

fedora devel list 의 스레드를 기반으로 2014 년에 systemd 및 OpenSSH에서 TCP 래퍼 지원을 제거한 것입니다 (중략..) 네트워킹 통신에 대한 위협이 지속적으로 증가하고 있지만이 패키지의 위협 범위는 지난 20 년 동안 동일하게 유지되어 새로운 위협이 현재 다른 구성 요소에 의해 처리되고 있다는 추론을 이끌어 냈습니다.

이전에 scp 관련한 포스팅과 유사하게 개발이 된지 오래된 라이브러리 패키지로 추가적인 기능 개선이 없었거나 더 좋은 도구(패키지)의 등장으로 인하여 대체 가능한 시점으로 판단되어 더 이상 지원을 하지 않기로 결정 된것 같습니다.

참조링크

- https://hoing.io/archives/14925
- https://access.redhat.com/solutions/3935901
- https://access.redhat.com/solutions/3906701
- https://access.redhat.com/solutions/6895291

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/tcp_wrapper

Last update: **2023/11/20 05:42**