OpenSSH Vulnerability CVE-2024-6387

An security vulnerability from openssh versions prior to 4.4p1 was re-introduced in openssh version 8.5p1 and fnially fixed again in version 9.8p1

The vulnerability allows an attacker to remotely execute code with root privileges without authentication, which is of course the worst case scenario of what could go wrong with openssh. However, the exploit is very complex to trigger as it is timing related and it requires a huge amount of trial and error, causing very high network traffic and is generally more likely to crash the openssh server than to actually succeed. For this reason Red Hat classified this vulnerability only as “Important” (level 3 out of 4). Still, it is highly recommended to mitigate or patch this vulnerability right away, as the damage that can be done through it is massive.

Links:

- Qualys FAQ
- Ubuntu Patch Status (ubuntu 22.04,23.10 and 24.04 have been patched, others are not affected, so bottom line: `apt-get update && apt-get upgrade` will do the trick for you)
- Rocky Linux 9 info and patch, requires adding another repo (8 is not affected)
- RedHat Enterprise Linux 9 info no patch provided, only below mitigation and info that only RHEL 9 is affected.

Mitigation

if no patch is available or you can't update for some reason, there is a mitigation method to make this attack impossible but it will make your ssh server more vulnerable to DoS attacks.

edit `/etc/ssh/sshd_config` and add or moify the following setting:

```
LoginGraceTime 0
```