CVE-2024-6387

Remote Code Execution via OpenSSH

Wat is CVE-2024-6387?

Kwetsbaarheid in **OpenSSH's sshd**

Race condition in SIGALRM handler

Remote Code Execution (RCE) zonder authenticatie

Aanval is **volledig automatisch uitvoerbaar**

Wat is de impact?

Volledige systeemovername

Kan elke OpenSSH-server raken (Linux, cloud, IoT)

Moeilijk op te sporen (race conditions = weinig logging)

Grote schaal mogelijk door automatisatie

Wat kan je doen?

Beperk toegang:

SSH ENKEL VIA VPN OF SPECIFIEKE IP’S

FAIL2BAN OF FIREWALL RATE LIMITING

Beveilig extra:

- LoginGraceTime inkorten
- MaxStartups verlagen
- Monitoring op SSH-activiteit
- SELinux of AppArmor activeren

Voorbereid zijn:

BACK-UPS, LOGGING
NAAR EXTERN SYSTEEM

PATCHBEHEER
AUTOMATISEREN

ZERO TRUST AANPAK