

CVE-2024-6387 – Remote Code Execution via OpenSSH

1 – Introductie

In dit document bespreken we **CVE-2024-6387**, een kritieke kwetsbaarheid in OpenSSH. We leggen uit wat deze kwetsbaarheid inhoudt, wat de impact ervan kan zijn voor organisaties en systemen, en welke maatregelen genomen kunnen worden om de schade te beperken of te voorkomen.

2 – Wat is CVE-2024-6387?

CVE-2024-6387 is een kwetsbaarheid in de **sshd**-component van **OpenSSH**.

Technische details:

- Het betreft een **race condition** in de **SIGALRM**-handler.
 - Hierdoor kan een aanvaller **remote code execution (RCE)** uitvoeren zonder dat er authenticatie nodig is.
 - De aanval werkt door duizenden verbindingen tegelijk op te zetten naar een SSH-server, in de hoop dat de race condition op het juiste moment optreedt.
 - De aanval is **volledig te automatiseren**, wat het risico op massale aanvallen vergroot.
-

3 – Wat is de impact?

De impact van deze kwetsbaarheid is zeer ernstig:

- Aanvallers kunnen **volledige toegang** krijgen tot het systeem als root.
 - De kwetsbaarheid treft vrijwel elke machine waarop OpenSSH draait, zoals Linux-servers, cloudomgevingen en IoT-apparaten.
 - Race conditions zijn **moeilijk te detecteren** omdat ze zelden duidelijke sporen nalaten in logbestanden.
 - Door de aard van de kwetsbaarheid is **massale exploitatie mogelijk**, vooral als systemen publiek toegankelijk zijn.
-

4 – Waarom updaten niet genoeg is

Hoewel **updaten** de primaire maatregel is, is dit in de praktijk niet altijd voldoende:

- In sommige omgevingen – zoals embedded systemen of legacy infrastructuur – kan patchen vertraagd of lastig zijn.
- Aanvallers zijn vaak sneller dan interne patchingprocessen.
- Alleen vertrouwen op updates is dus risicovol.

Een bredere beveiligingsaanpak is noodzakelijk.

5 – Wat kan je doen?

Om jezelf te beschermen tegen CVE-2024-6387, zijn er meerdere maatregelen mogelijk:

Beperk toegang:

- Laat SSH alleen toe via een **VPN** of via **specifieke IP-adressen**.
- Gebruik tools zoals **fail2ban** om brute-force aanvallen af te weren.
- Stel **firewall regels** in om verbindingen te beperken.

Beveilig extra:

- Verlaag de waarde van **LoginGraceTime** en **MaxStartups** in **sshd_config**.
- Activeer **monitoring** van SSH-activiteit en verbindingspogingen.
- Schakel **SELinux** of **AppArmor** in voor extra bescherming op systeemniveau.

Wees voorbereid:

- Zorg voor **regelmatige back-ups** en sla deze extern op.
- Gebruik een extern **logging systeem (SIEM)** om verdachte activiteiten op te sporen.
- Automatiseer **patchbeheer** en overweeg een **Zero Trust** beveiligingsmodel.

6 – Samenvatting

- CVE-2024-6387 is een ernstige kwetsbaarheid die **remote root access** mogelijk maakt zonder authenticatie.
- De aanval is moeilijk te detecteren en kan op grote schaal worden uitgevoerd.
- Een combinatie van **patching**, **toegangsbeperking**, **monitoring** en **defense-in-depth** is nodig om systemen te beschermen.