Vážná zranitelnost v OpenSSH

portal.nukib.gov.cz/informacni-servis/informace/upozorneni-a-hrozby/kriticka-zranitelnost-v-openssh

V OpenSSH, aplikaci pro vzdálenou správu převážně linuxových systémů, byla nalezena vážná zranitelnost, která dostala označení regreSSHion (CVE-2024-6387, CVSS 8.1). Útočník se vzdáleným přístupem k SSH serveru může zneužitím této zranitelnosti spouštět příkazy pod uživatelským účtem s maximálním oprávněním (root).

Ovlivněné verze touto zranitelností:

- verze 4.4p1 a starší jsou zranitelné na starší zranitelnosti CVE-2006-5051 a CVE-2008-4109, které jsou obdobné regreSSHion
- verze 4.4p1 až 8.5p1 (kromě) nejsou zranitelné
- verze 8.5p1 až 9.8p1 (kromě) jsou zranitelné

> NÚKIB zatím nedisponuje informacemi, že by tato zranitelnost byla aktivně zneužívána. Vzhledem ale k množství potenciálně napadnutelných systémů (v celém světě se jedná o 700 tisíc systémů) a kritičnosti se dá předpokládat, že útočníci budou tuto zranitelnost hromadně zneužívat v nejbližších dnech. **Proto doporučujeme co nejdříve akualizovat systémy, které zpřísupňují SSH pomocí zranitelné verze OpenSSH z Internetu.**

V případě, že není možné provést aktualizaci OpenSSH, je možné využít workaround a nastavit v konfiguračním souboru OpenSSH serveru hodnotu `LoginGraceTime 0`.

Verze OpenSSH v jednotlivých linuxových distribucích

- RHEL 9, CentOS 9, AlmaLinux 9: 8.7p1 – pravděpodobně zranitelná
- RHEL 8, CentOS 8, AlmaLinux 8: 8.0p1
- Ubuntu 24.04: 9.6p1 – pravděpodobně zranitelná
- Ubuntu 23.10: 9.3p1 – pravděpodobně zranitelná
- Ubuntu 22.04: 8.9p1 – pravděpodobně zranitelná

- Ubuntu 20.04: 8.2p1

Více informací

- https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server
- https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt
- https://security-tracker.debian.org/tracker/CVE-2024-6387
- https://access.redhat.com/security/cve/cve-2024-6387

Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

01. 07. 2024

Reakce

Zatím žádné reakce na článek