Backdoor v linuxových distribucích

V knihovně `xz` sloužící k kompresi souborů, která je standardní součásti téměř všech linuxových distribucí, byl objeden backdoor (zram, který do něj pravděpodobně umístil přímo autor knihovny. Tento backdoor umožňuje útočníkovi vzdálený přístup na linuxové systémy obsahující tuto knihovnu. Zranitelnost dostala označení CVE-2024-3094 (CVSS 10).

Backdoor se nachází ve verzích knihovny `xz` 5.6.0 (vydaná 24. dubna 2024) a 5.6.1 (vydaná 9. března 2024). Naštěstí linuxové distroubuci zavádí nové knihovny se zpožděním a postiženy jsou tak pouze nejnovější verze operačních systémů, které nejsou určeny k použití běžnými uživateli:

- Fedora Rawhide (nestabilní vydání Fedory)
- Fedora 41 (nestabilní vydání Fedory)
- Debian Sid (nestabilní vydání Debianu)
- Gentoo

(seznam není kompletní a může být dále rozšiřován)

V případě že používáte operační systém s postiženou verzí knihovny, výrobce doporučuje tento systém okamžitě přestat používat pro pracovní i soukromé účely.

Pro pracovní účely doporučujeme používat stabilní verze distribucí, kde se nové verze aplikací a knihoven dostávají se zpožděním a snižujete se tak riziko podobné zranitelnosti.

Zdroje

- https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users
- https://access.redhat.com/security/cve/CVE-2024-3094
- https://www.openwall.com/lists/oss-security/2024/03/29/4
- https://www.root.cz/clanky/sofistikovana-sabotaz-xz-se-pripravovala-roky-odhalena-byla-stastnou-nahodou/

Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

29. 03. 2024

Obsah

Reakce

Zatím žádné reakce na článek