Upozornění na aktivní zneužívání závažné zranitelnosti ve WinRAR (CVE-2023-38831)

portal.neweb.govcert.cz/informacni-servis/informace/upozorneni-a-hrozby/upozorneni-na-aktivni-zneuzivani-zavazne-zranitelnosti-ve-winrar-cve-2023-38831

Upozorňujeme na aktivní zneužívání závažné zranitelnosti ve WinRAR (CVE-2023-38831, CVSS 7.8), která byla zveřejněna v srpnu 2023, ovšem k výraznému zneužívání rusko-čínskými hackerskými skupinami dochází v měsících září a říjen. Zranitelnost se týká WinRAR 6.22 a starších verzí, ve kterých lze spustit škodlivý kód v okamžiku, kdy se uživatel pokusí zobrazit soubory v RAR archivu, které stáhnul z doručeného mailu. Nejčastěji se jedná o sadu souborů JPEG a PNG, mezi kterými se nachází soubor napodobující obrazový formát obsahující libovolný kód, například „poc.png .cmd“ (mezera je zde záměrná). Alternativně se lze setkat s variantou napodobující PDF soubor. Doporučujeme aktualizovat verzi WinRAR na nejnovější **verzi 6.24**.

Odkazy

- https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/
- https://consent.yahoo.com/v2/collectConsent?sessionId=3_cc-session_66037db8-3a9f-413f-ab20-fcd6a40b9aef
- https://www.bleepingcomputer.com/news/security/google-links-winrar-exploitation-to-russian-chinese-state-hackers/
- https://nvd.nist.gov/vuln/detail/CVE-2023-38831

Klasifikace

TLP:GREEN

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

20. 10. 2023

Obsah

Reakce

Zatím žádné reakce na článek