NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BEZPEČNOSTNÉ VAROVANIE

No: V20230217-03K

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

OpenSSH Server - kritická bezpečnostná zraniteľnosť

Popis

Vývojári nástroja OpenSSH Server vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť.
Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

08.02.2023

CVE

CVE-2023-25136

Zasiahnuté systémy

OpenSSH vo verzii staršej ako 9.2p1

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://seclists.org/oss-sec/2023/q1/92
https://nvd.nist.gov/vuln/detail/CVE-2023-25136
https://www.openssh.com/txt/release-9.2
https://jfrog.com/blog/openssh-pre-auth-double-free-cve-2023-25136-writeup-and-proof-of-concept/
https://bugzilla.mindrot.org/show_bug.cgi?id=3522
https://blog.qualys.com/vulnerabilities-threat-research/2023/02/03/cve-2023-25136-pre-auth-double-free-vulnerability-in-openssh-server-9-1
https://thehackernews.com/2023/02/openssh-releases-patch-for-new-pre-auth.html

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava
Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915
SK-CERT
Naša značka:
01794/2022/SK-CERT-1038