NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Č.: 08031/2023/SRD/ORM-002 Bratislava 12.06.2023

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 5 ods. 1 písm. q) v spojení s § 27 ods. 1 písm. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

v y h l a s u j e

VAROVANIE

pred hrozbou vzniku závažných kybernetických bezpečnostných incidentov z dôvodu výskytu novej kritickej zraniteľnosti v operačnom systéme FortiOS, ktorý je súčasťou rôznych produktov spoločnosti Fortinet. Produkty spoločnosti Fortinet sú široko používané organizáciami v slovenskom kybernetickom priestore vrátane prevádzkovateľov základných služieb.

Zraniteľnosť sa nachádza v používateľskom webovom rozhraní pre SSL VPN (nie v administračnom rozhraní) a týka sa všetkých zariadení s iným než aktuálnym firmvérom, ktoré majú VPN port sprístupnený na internete. Je predpoklad, že na jej zneužitie nie je potrebné, aby služba SSL VPN ako taká bola na zariadení využívaná. Zneužitie zraniteľnosti umožňuje **vzdialené vykonanie kódu** a úplné narušenie dôvernosti, integrity a dostupnosti.

Zraniteľnosť ešte nebola oficiálne ohlásená výrobcom, je však široko komunikovaná v bezpečnostnej komunite a je jej pridelené **číslo CVE-2023-27997**. **Oprava tejto zraniteľnosti sa nachádza v najnovších verziách 6.0.17, 6.2.15, 6.4.13, 7.0.12, 7.2.5**, vydaných v piatok 9. júna 2023. Očakáva sa, že výrobca sa k nej oficiálne vyjadrí v utorok 13. júna 2023. Národné centrum kybernetickej bezpečnosti (SK-CERT) odhaduje, že táto zraniteľnosť môže dosiahnuť CVSS skóre až 10.0.

Túto zraniteľnosť je možné zneužiť **bez akejkoľvek autentifikácie**, preto jej nezabráni ani správne nastavená viacfaktorová autentifikácia.

Úrad v súvislosti s touto hrozbou dôrazne odporúča prijať nasledujúce opatrenia:

- **bezodkladne** aktualizovať firmvér na najnovšiu dostupnú verziu, najmenej však **na verzie 6.0.17, 6.2.15, 6.4.13, 7.0.12, 7.2.5**. Ak aktualizácia nie je možná, **zariadenie vypnite**. V tomto prípade sa odporúča nečakať do pravidelného aktualizačného okna vzhľadom k mimoriadnemu riziku,
- po aktualizácii **zmeniť** všetky kľúče, heslá a VPN prístupy na zasiahnutom zariadení,
- v logoch zariadení na lokálnej sieti (servery, pracovné stanice) vyhľadať vnútorné adresy zasiahnutého zariadenia a posúdiť, či ide o legitímnu komunikáciu. Ak nájdete podozrivé spojenia (napr. skenovanie portov, pokusy o prihlásenie, enumeráciu webových aplikácií), **predpokladajte kompromitáciu** a odštartujte plnú reakciu na incident,
- ak je to možné, na nezávislom zariadení identifikovať sieťové spojenia z Internetu na SSL VPN a porovnať s legitímnymi pripojeniami používateľov. Ak takto identifikujete komunikáciu s externou IP adresou, ktorá nepatrila legitímnemu VPN pripojeniu, a v rámci spojenia bolo prenesených viac než 10 kB dát, **predpokladajte kompromitáciu** a odštartujte plnú reakciu na incident,
- prípadný incident **nezabudnite nahlásiť** Národnému centru kybernetickej bezpečnosti SK-CERT na adrese incident@nbu.gov.sk.