TLP:WHITE
Szabadon terjeszthető!

Riasztás
FortiOS és FortiProxy szoftverek kritikus kockázati besorolású sérülékenységéről

(2023. június 13.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) **riasztást** ad ki a **Fortigate tűzfal termékek FortiOS** és **FortiProxy SSL-VPN** komponensét érintő **kritikus kockázati besorolású** sérülékenység kapcsán, annak súlyossága, feltételezett kihasználtsága, valamint a Fortigate termékek széleskörű elterjedtsége miatt.

A **CVE-2023-27997**[1] azonosítón nyomon követett biztonsági hiba abban az esetben használható ki, amennyiben az **SSL-VPN funkció engedélyezve van** a sérülékeny verziót futtató eszközön. Egy támadó sikeres kihasználás esetén speciálisan szerkesztett kérésekkel a hitelesítést megkerülve, távolról tetszőleges kódot futtathat a sérülékeny eszközön.

A Fortigate 2023.06.12-ei biztonsági közleménye[2] szerint egy kódaudit során fedezték fel a **CVE-2023-27997** (a Fortinet **FG-IR-23-097**[3] azonosítójú) sérülékenységet, és a sebezhetőség aktív kihasználására utaló jeleket is tapasztaltak. A gyártó felhívja a figyelmet arra, hogy termékei különböző fenyegetési szereplők célkeresztjébe kerülhetnek, amint arra korábban is volt példa a „Volt Typhoon" APT csoport részéről.[4]

Érintett termékek és verziók:

FortiOS-6K7K	**7.0.10; 7.0.5; 6.4.12; 6.4.10; 6.4.8; 6.4.6; 6.4.2; 6.2.9 - 6.2.13; 6.2.6 - 6.2.7; 6.2.6 - 6.2.7; 6.2.4; 6.0.12 - 6.0.16; 6.0.10**
FortiProxy	**7.2.0 - 7.2.3; 7.0.0 - 7.0.9; 2.0.0 - 2.0.12; 1.2 (minden alverzió); 1.1 (minden alverzió)**
FortiOS	**7.2.0 - 7.2.4; 7.0.0 - 7.0.11; 6.4.0 - 6.4.12; 6.0.0 - 6.0.16**

Hibajavítást tartalmazó verziók:

FortiOS-6K7K	**7.0.12 (vagy ennél frissebb verzió);** **6.4.13 (vagy ennél frissebb verzió);** **6.2.15 (vagy ennél frissebb verzió);** **6.0.17 (vagy ennél frissebb verzió)**
FortiProxy	**7.2.4 (vagy ennél frissebb verzió);**

	7.0.10 (vagy ennél frissebb verzió); **2.0.13 (vagy ennél frissebb verzió)**
FortiOS	**7.4.0 (vagy ennél frissebb verzió);** **7.2.5 (vagy ennél frissebb verzió);** **7.0.12 (vagy ennél frissebb verzió);** **6.4.13 (vagy ennél frissebb verzió);** **6.2.14 (vagy ennél frissebb verzió);** **6.0.17 (vagy ennél frissebb verzió)**

Javaslatok

- **Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítéssel, valamint manuálisan is letölthetők a gyártói honlapokról.**
- **A gyártói közlemény alapján javasolt a Fortigate termékek korábbi sebezhetőségeivel[4] összefüggésbe hozható indikátorok alapján kiterjedt vizsgálatot folytatni az esetleges kompromittáltság felderítéséhez.**
- **A FortiOS biztonsági hardeningje a gyártói útmutató[5] alapján.**
- **A támadási felület csökkentése érdekében az SSL-VPN funkció tiltása.**

Hivatkozások:

1. https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/cve-2023-27997/
2. https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign
3. https://www.fortiguard.com/psirt/FG-IR-23-097
4. https://www.fortiguard.com/psirt/FG-IR-22-377
5. https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/555436/hardening
6. https://nki.gov.hu/it-biztonsag/hirek/meg-nem-dokumentalt-kritikus-serulekenyseg-kerult-javitasra-fortigate-ssl-vpn-eszkozokben/

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu