

Upozorňujeme na kritickou zranitelnost FortiOS CVE-2023-27997

portal.newweb.govcert.cz/informacni-servis/upozorneni-a-hrozby/upozornujeme-na-kritickou-zranitelnost-fortios-cve-2023-27997

Upozorňujeme na remote code execution (RCE) zranitelnost CVE-2023-27997 ve FortiOS (operační systém používaný mimo jiné v firewallech Fortigate) od společnosti Fortinet v SSL-VPN, která útočnickovi umožňuje operovat s VPN připojením i přes zapnuté dvoufaktorové ověření, jelikož pro její zneužití není potřeba autentizace.

Více informací o této zranitelnosti oznámí společnost Fortinet v úterý 13. června 2023. Zatím není znám přesný dopad zranitelnosti a možnosti detekce jejího zneužití. Po obdržení více informací budeme tento článek aktualizovat.

V tuto chvíli doporučujeme okamžitý update FortiOS na jednu z následujících verzí: 7.2.5, 7.0.12, 6.4.13, 6.2.15, 6.0.17. V těchto verzích je již zranitelnost opravena. Aktualizace byla vydána i pro řadu 6.0, pro kterou již výrobce oficiálně neposkytuje podporu. Tato aktualizace byla vydána 9. června 2023.

Zdroje

<https://www.helpnetsecurity.com/2023/06/11/cve-2023-27997/>