Záplaty Fortinet předautorizují RCE, aktualizujte své firewally Fortigate ASAP! (CVE-2023-27997)

helpnetsecurity.com/2023/06/11/cve-2023-27997

11. června 2023

Společnost Fortinet vydala několik verzí FortiOS, OS/firmwaru napájejícího firewally Fortigate a další zařízení, aniž by zmínila, že zahrnují opravu CVE-2023-27997, chyby vzdáleného spouštění kódu (RCE), která nevyžaduje, aby byl útočník přihlášeni, abyste to mohli využít.

Zranitelnost byla opravena ve verzích FortiOS 7.2.5, 7.0.12, 6.4.13, 6.2.15 a zjevně také ve verzi 6.0.17 (i když Fortinet v loňském roce oficiálně přestal podporovat větev 6.0).

Podnikovým správcům se doporučuje upgradovat zařízení Fortigate co nejdříve – pokud tuto zranitelnost již útočníci nezneužívají, je pravděpodobné, že brzy bude.

O CVE-2023-27997

Přesná povaha zranitelnosti je v současnosti (veřejně) neznámá. Podle Olympe Cyberdefense společnost Fortinet zveřejní další podrobnosti 13. června 2023 (úterý).

Říká se, že zranitelnost je kritická, ovlivňuje funkčnost SSL VPN Fortigate firwall a může útočníkovi umožnit „zasahovat přes VPN, i když je aktivováno MFA“.

Bezpečnostní výzkumník společnosti Lexfo Charles Fol, který spolu s kolegou Dany Bachem nahlásili chybu, říká , že CVE-2023-27997 umožňuje RCE, je „dosažitelná předběžná autentizace na každém zařízení SSL VPN“ a že další podrobnosti zveřejní na Později.

V současné době není žádná zmínka o možných řešeních.

Rychle opravte!

Bohužel pro obránce podniků mohou aktéři hrozeb porovnat novější verze operačního systému se staršími, aby zjistili, co oprava dělá, a na základě těchto informací vyvinout funkční exploit.

Zranitelnosti ovlivňující firewally Fortigate byly v minulosti oblíbeným cílem .

Fortinet je také známý tím, že tlačí kritické opravy, aniž by zmiňoval zranitelnosti – ať už jsou aktivně využívány, nebo ne. Podnikoví administrátoři by proto měli postupovat rychle a implementovat opravu co nejdříve.

Pokud se dostupná aktualizace nezobrazí na řídicím panelu zařízení, může se zobrazit až po restartování. Pokud ne, doporučujeme ruční stažení a instalaci.