Kritická zranitelnost Palo Alto PAN-OS (aktualizováno 15. 4.)

> Aktualizováno 15. 4.: Oprava na kritickou zranitelnost CVE-2024-3400 (CVSS 10) byla již vydána v neděli 14. 4. Více informací naleznete na https://security.paloaltonetworks.com/CVE-2024-3400

Společnost Palo Alto Networks vydala aktualizace firewallů s operačním systémem PAN-OS. Aktualizace opravuje několik středně a vysoce závažných bezpečnostních chyb a je doporučeno aplikovat aktualizace bez zbytečného odkladu.

Jedná se především o tři zranitelnosti, které je možné zneužít k útoku DoS (denial-of-service). Chyba CVE-2024-3385 (CVSS 7.5) se týká pouze firewallů PA-5400 a PA-7000 pokud je zakázáno zabezpečení GTP. Chyba CVE-2024-3384 (CVSS 7.5) umožňuje pomocí speciálně vytvořených paketů NTLM firewall vzdáleně přepnout do režimu údržby, který vyžaduje ruční zásah k obnovení systému. Třetí chybou je CVE-2024-3382 (CVSS 7.5), která umožňuje útočníkovi zahltit firewall zasíláním množství škodlivých paketů, což mu brání ve zpracování legitimního provozu. Tato chyba se týká pouze zařízení s povolenou funkcí SSL Forward Proxy.

Čtvrtou závažnou chybou je CVE-2024-3383 (CVSS 7.4) související se způsobem zpracování dat přijatých od agentů Cloud Identity Engine (CIE). Lze zneužít k úpravě skupin User-ID a má tak dopad na oprávnění uživatelů k síťovým zdrojům (odepření legitimních nebo zpřístupnění nelegitimních zdrojů pomocí stávajících bezpečnostních pravidel).

Společnost Palo Alto Networks také informovala o chybě CVE-2024-3400 (CVSS 9.8), týkající se verzí systému PAN-OS 10.2, PAN-OS 11.0 nebo PAN-OS 11.1. Ta umožňuje vzdálené vkládání příkazů neověřenému útočníkovi a získat tak přístup k zařízení a spustit libovolný kód s oprávněním ROOT. Na tuto zranitelnost bude vydána opravná aktualizace až 14. 4. Do té doby je možné zmírnit zranitelnost vypnutím „Enable Telemetry“ v nastavení zařízení. Dle informací výrobce je tato zranitelnost již aktivně zneužívána.

Zdroje

- https://www.securityweek.com/palo-alto-networks-patches-vulnerabilities-allowing-firewall-disruption/
- https://security.paloaltonetworks.com/CVE-2024-3400
- https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_12/2024

Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

12. 04. 2024

Obsah

Reakce

Zatím žádné reakce na článek