Upozornění na dvě kritické zranitelnosti FortiOS (aktualizováno)

V operačním systému FortiOS používaném ve firewallech FortiGate od společnosti Fortinet byly opraveny dvě kritické zranitelnosti, které jsou vzdáleně zneužitelné. Jedna z nich je již aktivně zneužívána. **Doporučujeme neprodleně provést aktualizaci všech zranitelných produktů od této společnosti.** V případě, že firewally nenabízí provedení aktualizace, je nutné ji stáhnout přímo z webu výrobce.

> V této souvislosti si dovolujeme dále upozornit, že FortiOS řady 6.2 již není výrobcem podporován, i když pro zranitelnost CVE-2024-21762 byla vydána opravená verze. Podpora pro řadu 6.4 skončí 30. září 2024.

Zranitelnost CVE-2024-21762 (CVSS 9.6)

Tato zranitelnost v SSL VPN, která **je již aktivně zneužívána**, umožňuje vzdálenému útočníkovi i bez autentizace spouštět na zranitelném zařízení jakékoliv příkazy systému.

Pro mitigaci je nutné provést aktualizaci systému nebo vypnout SSL VPN.

Zranitelné jsou všechny verze 6.0–7.4, pro nepodporovanou řadu 6.0 aktualizace nebyla vydána.

Více informací

Zranitelnost CVE-2024-23113 (CVSS 9.8)

Zranitelnost se týká součásti fgfmd, kdy zneužitím této zranitelnosti vzdálený neautentizovaný útočník může útočník na zranitelném zařízení spouštět jakékoliv příkazy systému.

Pro mitigaci je nutné provést aktualizaci systému.

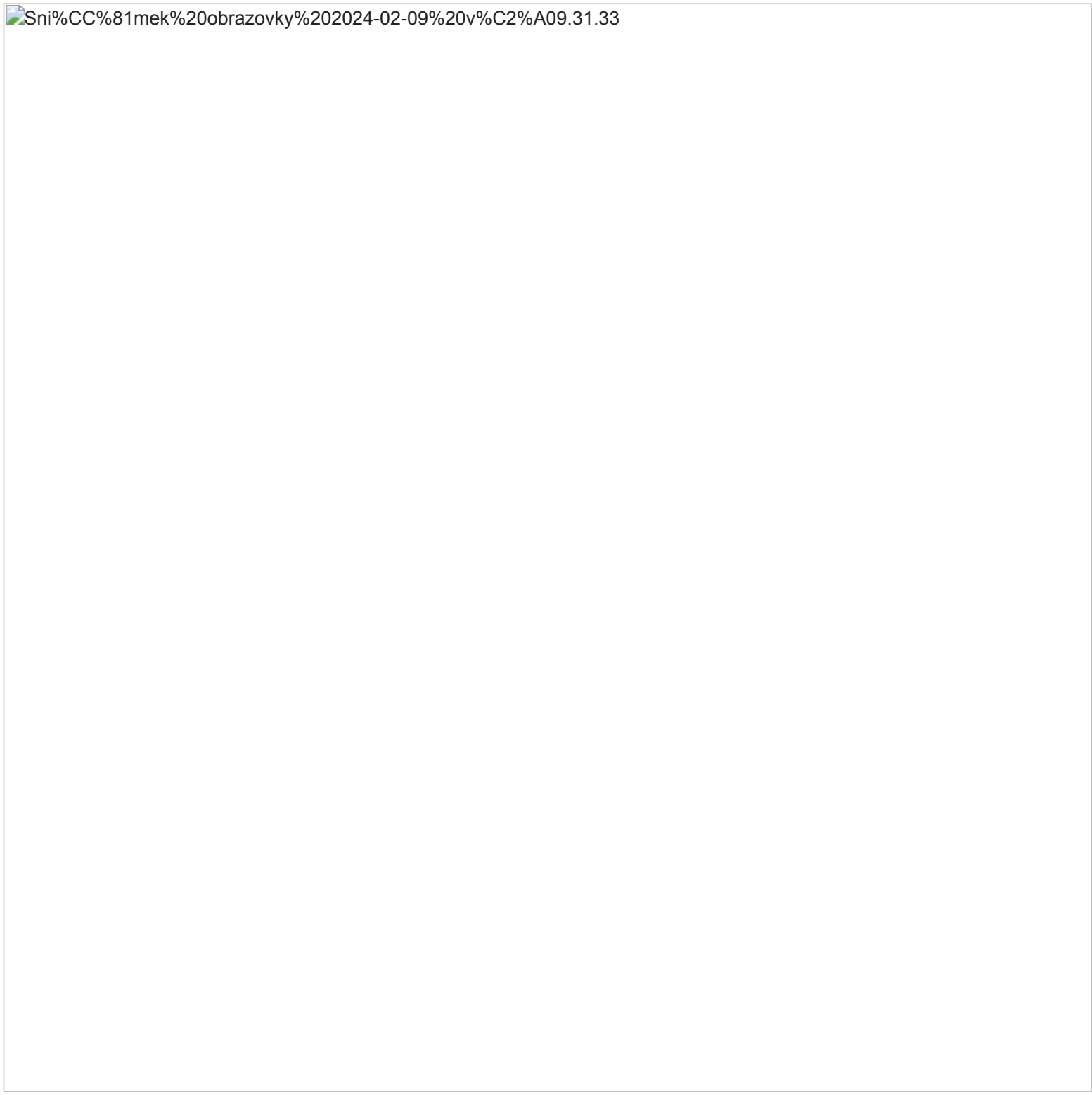
Zranitelné jsou všechny verze 7.0-7.4, řada 6.X touto zranitelností není postižena.

Více informací

Opravené verze FortiOS

- 6.2.16 Build 1392
- 6.4.15 Build 2095
- 7.0.14 Build 0601
- 7.2.7 Build 1577
- 7.4.3 Build 2573

Tabulka podpory řad FortiOS



Klasifikace

TLP:CLEAR

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

08. 02. 2024

Reakce

7