UPOZORNĚNÍ NA NOVÉ HROZBY PRO OCHRANU OSOBNÍCH ÚDAJŮ

Úřad pro ochranu osobních údajů vydal upozornění na nové hrozby, a to nejen pro ochranu osobních údajů. Správci by proto měli provést taková opatření, aby zamezili nebezpečí napadení, a tím i potenciálního porušení zabezpečení osobních údajů.

Byly indikovány nové hrozby, a to nejen pro ochranu osobních údajů. Správci by proto měli provést taková opatření, aby zamezili nebezpečí napadení, a tím i potenciálního porušení zabezpečení osobních údajů.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) varuje před novou hrozbou phishingových podvodů, tentokrát s motivem nabídky příspěvku na bydlení od Ministerstva práce a sociálních věcí (MPSV). Cílem je přesvědčit adresáty k přihlášení na podvodné stránce pomocí bankovní identity. Zadané přihlašovací údaje pak útočníci aktivně využijí k přihlášení do legitimního bankovnictví, a tím dojde k odeslání výzvy pro dvoufázové ověření, kterou v tu chvíli oběť potvrdí.

Zároveň s tím byla ze strany NÚKIB indikována závažná zranitelnost pro vzdálené připojení VPN. Zranitelnost CVE-2022-26113 (CVSS 7.5), která se týká vzdáleného připojení klienta do vnitřní sítě. Neprivilegovanému uživateli, který disponuje přístupem ke koncové stanici s VPN klientem od společnosti FortiClient, je umožněno získat práva uživatele SYSTEM.

Zranitelné jsou následující verze klienta pro operační systém Windows

- FortiClientWindows verze od 6.0.0 do 6.0.10
- FortiClientWindows verze od 6.2.0 do 6.2.9
- FortiClientWindows verze od 6.4.0 do 6.4.7
- FortiClientWindows verze od 7.0.0 do 7.0.3

Pro snížení škodlivosti následků této zranitelnosti je nutné aktualizovat na FortiClientWindows verze 7.0.4 a vyšší nebo verze 6.4.8 a vyšší.

Pokud k napadení dojde prostřednictvím softwarové aplikace, na jejíž zranitelnost upozornil např. Národní úřad pro kybernetickou a informační bezpečnost a správce neučinil doporučené kroky pro zajištění odpovídající ochrany osobních údajů, může to být hodnoceno jako porušení povinností správce, protože varování bylo publikováno před případným kybernetickým napadením.