UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Centrum informačných a komunikačných technológií

**Úsek informačnej a kybernetickej bezpečnosti**
**Tím na riešenie počítačových bezpečnostných incidentov (CSIRT-UPJS)**
Šrobárova 2, 041 80 Košice
VoIP: +421 (055) 234 2425, IČO: 00397768
csirt@upjs.sk, https://csirt.upjs.sk/

**TLP:CLEAR**

# Týždenná správa csirt.upjs.sk
# 14.1.2025 – 17.1.2025

**TLP:CLEAR**

## Vypracoval: csirt.upjs.sk

## Google OAuth zraniteľnosť ohrozuje milióny používateľov prostredníctvom opustených domén

Výskumníci odhalili zraniteľnosť v "Sign in with Google", ktorá umožňuje útočníkom získať prístup k účtom prostredníctvom odkúpenia neaktívnych domén. Google OAuth používa prístupový token na overenie identity používateľa. Ak sa služba spolieha len na údaje ako e-mail a hostovaná doména, zmena vlastníctva domény umožní neoprávnený prístup. Truffle Security upozornila na nespoľahlivosť sub claim v Google OAuth, ktorý mal identifikovať používateľa. Microsoft Entra využíva lepšie riešenie prostredníctvom sub/oid claims, ktoré sú nemenné. Google najprv označil správanie za zamýšľané, ale neskôr priznal problém a odmenil výskumníka.

## Únik údajov z Fortinet zariadení

Na dark webe bolo zverejnených vyše 15 000 konfigurácií Fortinet zariadení vrátane prihlasovacích údajov pre VPN. Únik sa týkal zariadení zraniteľných voči chybe **CVE-2022-40684**, ktorá umožňovala neoprávnený administratívny prístup. Údaje pochádzajú spred viac ako dvoch rokov, no zariadenia bez aktualizácií sú stále ohrozené. Fortinet nedávno odhalil novú zraniteľnosť **CVE-2024-55591**, ktorá zdôrazňuje nutnosť pravidelných aktualizácií.

## Útočníci zneužívajú Google reklamy na krádež účtov Google Ads

Hackeri používajú Google Search reklamy na propagáciu phishingových stránok, ktoré kradnú prihlasovacie údaje Google Ads účtov. Sponzorované odkazy vedú na falošné prihlasovacie stránky hostované na Google Sites, čím zvyšujú dôveryhodnosť útoku. Používajú phishingové kity na zhromaždenie prihlasovacích údajov, cookies a ďalších identifikátorov. Po získaní údajov pridajú útočníci nového administrátora a môžu obeť z účtu zablokovať. Útoky vedú k finančným stratám a strate kontroly nad reklamnými kampaňami.

## Kritické chyby v prepínačoch Planet WGS-804HPT umožňujú vzdialené útoky

Výskumníci odhalili tri závažné zraniteľnosti v prepínačoch Planet WGS-804HPT, ktoré umožňujú vzdialené spustenie kódu bez autentifikácie. Zraniteľnosti zahŕňajú chybu podtečenia celého čísla (CVE-2024-52558), injekciu príkazov (CVE-2024-52320) a pretečenie zásobníka (CVE-2024-48871). Tieto chyby umožňujú útočníkovi vykonávať príkazy operačného systému a prevziať kontrolu nad zariadením. Útoky sú zamerané na rozhranie dispatcher.cgi, ktoré poskytuje webovú službu. Prepínače sa používajú v systémoch automatizácie budov, čo zvyšuje riziko sieťových útokov. Planet Technology vydala opravu v verzii 1.305b241111 dňa 15. novembra 2024.

## Zraniteľnosť v macOS umožňuje inštaláciu rootkitov

Microsoft odhalil chybu CVE-2024-44243, ktorá umožňuje obísť System Integrity Protection (SIP) v macOS a nainštalovať škodlivé kernelové ovládače. SIP je bezpečnostný mechanizmus, ktorý chráni systém pred modifikáciou aj s oprávneniami "root". Chyba sa nachádza v démonovi storagekitd, ktorý má špeciálne oprávnenia. Útočník môže manipulovať s adresárom /Library/Filesystems a nahradiť systémové binárne súbory. To umožňuje spustenie malvéru, obídenie Transparency, Consent and Control (TCC) a vytvorenie trvalého rootkitu. Apple problém opravil v aktualizácii macOS Sequoia 15.2.