MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Apríl 2023

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci apríl riešil štandardne najmä phishingové kampane zasahujúce jeho konštituenciu. Vyskytli sa tiež prípady kompromitovaných e-mailových účtov zamestnancov verejných inštitúcií, z ktorých útočníci rozposielali phishingové e-maily na ďalšie organizácie v konštituencii CSIRT.SK.

CSIRT.SK prijal v apríli informácie o útokoch typu DDoS na webové sídla MV SR (www.minv.sk), ŽSR (www.zsr.sk) a streamovacie služby RTVS. Iba pri útoku na ŽSR bola ako útočník potvrdená proruská hacktivistivká skupina NoName057(16).

Jednotka získala tiež informácie o pokuse o zneužitie zraniteľností MS Exchange CVE-2022-41040 a CVE-2022-41082 na mailserveri serveri organizácie vo svojej konštituencii. Zraniteľnosti umožňujú útočníkom získať vyššie oprávnenia a vzdialene vykonávať kód. Zaznamenané boli tiež pokusy o prienik do infraštruktúry ďalšej organizácie. Techniky, ktoré útočníci skúšali, boli zneužitie zraniteľnosti Log4Shell, path traversal, cross site scripting (XSS) a SQL injection.

CSIRT.SK riešil tiež v rámci svojej konštituencie medializovaný incident, pri ktorom utrpela spoločnosť Datalan škody spôsobené ransomvérom. Spoločnosť poskytuje služby mnohým organizáciám verejnej správy a incident mohol viesť k úniku prihlasovacích údajov k VPN prístupom do infraštruktúr klientov a ďalších služieb. Vzhľadom na túto možnosť kontaktoval CSIRT.SK organizácie vo svojej konštituencii a poskytol im odporúčania a pomoc v prípade potreby. Žiadne škody však neboli nahlásené.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií vo svojej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje. Jednotka rozšírila svoj monitoring o nedostupné webové domény.

Mesačník zraniteľností apríl 2023

CSIRT.SK vydáva a uverejňuje na svojej stránke prehľad kritických zraniteľností bežného softvérového vybavenia na mesačnej báze. Jedná sa o nasledovné produkty:

1. Operačné systémy Microsoft Windows
2. Kancelárske balíky Microsoft Office a Office Web Apps
3. Internetové prehliadače
    - Microsoft Internet Explorer
    - Microsoft Edge
    - Mozilla Firefox
    - Google Chrome
4. Adobe Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohto mesačné závažné zraniteľnosti
    - Android
    - VMware vRealize (Aria)

https://www.csirt.gov.sk/posts/3385.html?csrt=17713649575071023780