MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Apríl 2022

(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 kompromitácie e-mailového konta.

Jednotka pokračovala v riešení prípadu rozsiahlej spear-phishingovej kampane spojenej s únikom legitímnej komunikácie medzi viacerými organizáciami v konštituencii CSIRT.SK, aj súkromných spoločností. O kampani jednotka informovala aj na svojej webovej stránke. Útočníci zneužívali ukradnuté správy pri tvorení spear-phishingových e-mailov s odkazom na škodlivý súbor. Phishingovú časť priložili do vlákna ako odpoveď na túto komunikáciu a posielali ju pôvodným adresátom. Týmto spôsobom získali phishingové správy vyššiu dôveryhodnosť. Jednotka preverila pravdepodobné miesta úniku, korelovala domény adresátov vo vláknach legitímych častí nahlásených e-mailov a dospela ku zdroju úniku. Forenzné vyšetrovanie odhalilo, že útočníci pre exfiltráciu komunikácie zneužili zraniteľnosti mailserverov Microsoft Exchange (CVE-2021-26855 (ProxyLogon) a CVE-2021-34473 (ProxyShell)). Aplikácia opravnej aktualizácie korelovala so zastavením únikov e-mailov. Doručenie podvodných e-mailov v rámci tejto kampane nahlásilo jednotke CSIRT.SK viacero organizácií štátnej a verejnej správy.

V apríli bol vládnej jednotke CSIRT ohlásený ransomvérový incident, ktorý zasiahol dva fyzické servery v infraštruktúre zasiahnutej organizácie. Zariadenia obsahovali intranet vrátane registratúry, Active Directory a mailserver organizácie.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK ďalej vykonáva pravidelné skenovanie a overovanie zraniteľností v službách a zariadeniach IT infraštruktúr organizácií v jej konštituencii, ktoré sú vystavené do internetu. Využíva k tomu platformu Achilles, ktorú sama vyvíja a prevádzkuje.

Mesačník zraniteľností Apríl 2022

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 tohtomesačné závažné zraniteľnosti
    - Spring Framework - Spring4Shell
    - Gitlab
    - SonicWall SonicOs
    - OpenSSL
    - Nginx

https://www.csirt.gov.sk/posts/2888.html?csrt=1258759518691427888