MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Október 2023

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

Október bol vzhľadom na závažnosť incidentov nahlásených CSIRT.SK pomerne pokojným mesiacom. V rámci svojej bežnej činnosti CSIRT.SK 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. Kontinuálne pozorujeme spearphishingovú kampaň, v ktorej sa útočníci vydávajú za vedúceho zamestnanca obete a požadujú prevod väčšej sumy na zahraničné účty.

Významnejším incidentom okrem phishingových, ktorý bol nahlásený jednotke CSIRT.SK, bol útok typu DDoS na webové služby slovensko.sk a data.gov.sk v správe NASES.

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. Vo februári navyše informovala majiteľov zraniteľných MS Exchange serverov o vydaní opravy vysoko závažnej zraniteľnosti CVE-2023-21707, ktorá umožňuje vzdialene vykonávať kód.

Mesačník zraniteľností október 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
    - Atlassian Confluence
    - Cisco IOS XE
    - Apple
    - Zoho ManageEngine a FortiOS SSL-VPN (zneužité zraniteľnosti)

https://www.csirt.gov.sk/posts/3826.html?csrt=7216140814539333579