MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

September 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 september 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.

Jednotka CSIRT.SK prijala hlásenie ransomvérového útoku na základnú školu. Zasiahnuté boli dva servery a päť používateľských PC. Záložné NAS nerozpoznávalo obsah na svojich diskoch. Počas analýzy a riešenia incidentu sa jednotke podarilo obnoviť všetky stratené dáta. Škola dostane tiež odporúčania pre vybudovanie novej, bezpečnejšej sieťovej infraštruktúry.

Vládna jednotka CSIRT prijala tiež hlásenie kurióznej zraniteľnosti na webových stránkach organizácie. Webová aplikácia bola zverejnená v debug móde, čo umožňovalo voľný prístup k nešifrovaným citlivým dátam vrátane hesiel.

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 september 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
    - Junos OS
    - NAS Western Digital a Synology
    - Foxit PDF Editor a Reader
    - FortiOS

https://www.csirt.gov.sk/posts/3666.html?csrt=11741655256198314795