MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Júl 2023

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

Mesiac júl sa v súvislosti s nahlásenými závažnými kybernetickými útokmi na organizácie štátnej a verejnej správy niesol v pokojnejšom duchu.

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci júl 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.

Pokračovala spear-phishingová kampaň na ministerstvá zahraničných vecí viacerých krajín, vedená pravdepodobne ruskou skupinou APT29, známou tiež pod názvom Sandworm.

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 júl 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
    - FortiOS, FortiProxy
    - SAP Business Client, SAP ECC, SAP S/4HANA
    - Zimbra Collaboration Suite
    - Ubiquiti EdgeRouter a AirCube
    - Technicolor DSL TG670
    - Apple iOS, macOS, watchOS, Safari

https://www.csirt.gov.sk/posts/3525