MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

August 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 august 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. Okrem toho bol nahlásený prípad brute-force útoku na OWA organizácie, ktorý spôsobil zablokovanie napadnutých účtov, bez úspešného prístupu. Nahlásené boli aj prípady uniknutých prihlasovacích údajov ponúkaných na útočníckych fórach na darkwebe.

Jednotka zachytila pokračujúcu spearphishingovú kampaň, v ktorej sa útočníci vydávajú za vedúceho zamestnanca obete a požadujú prevod väčšej sumy na zahraničné účty. Objavila sa tiež spear-phishingová kampaň s cieľom získať od obetí potvrdenie dát o cieľovej organizácii v systéme pre TED Europe, vestníku pre verejné obstarávania.

Najzávažnejším incidentom, ktorého nahlásenie vládna jednotka CSIRT v auguste prijala, bol ransomvérový útok na Úrad košického samosprávneho kraja. Útok zasiahol značnú časť serverov organizácie. Jednotka urobila výjazd na miesto pre zaistenie forenzných stôp a jej špecialisti začali ich forenznú analýzu.

V auguste sa odohral ďalší útok DDoS, cielený na zneprístupnenie webstránok niektorých slovenských organizácií. Aktérom bola skupina hacktivistov Noname057(16). Ich cieľom sa stalo Ministerstvo obrany SR (www.mosr.sk), Ministerstvo zahraničných vecí a európskych záležitostí SR (www.foreign.gov.sk), Ministerstvo vnútra SR (www.minv.sk) a spoločnosť Konštrukta Defence (kotadef.sk).

Jendotka riešila aj kompromitáciu systému, kde útočník zneužil zraniteľnosť frameworku Symphony a nahral jednoduchý shell na zraniteľný server.

CSIRT.SK zachytil tiež informáciu o výhražných e-mailoch o nastražení bomby v budove, ktoré boli doručené na niekoľko organizácií. Správy odoslal útočník z anonymizačnej platformy pre hromadné rozposielanie e-mailov.

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. V auguste navyše informovala organizácie štátnej a verejnej správy kampani výhražných e-mailov, spomínaných vyššie.

Mesačník zraniteľností august 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
    - Joe Sandbox
    - Mikrotik, RouterOS

https://www.csirt.gov.sk/posts/3635.html?csrt=11741655256198314795