MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Február 2024

(skrátená verzia)

Vypracoval: CSIRT.SK

TLP: White

Riešené incidenty na Slovensku a z našej činnosti

V rámci svojej bežnej činnosti CSIRT.SK v mesiaci február 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 sa naďalej stretávala s phishingovou kampaňou zameranou na občanov Slovenskej republiky, v ktorej útočníci predstierajúci totožnosť Europolu a vysokopostavených členov Polície SR. Útočníci tentokrát z adries služby Gmail posielajú svojim obetiam falošné predvolania kvôli prechovávaniu detskej pornografie a podobným sexuálnym deliktom.

Vládna jednotka CSIRT prijala hlásenie zraniteľnej webstránky organizácie v jej konštituencii, ktorá mohla viesť k úniku citlivých údajov. Správca hlásenie vyriešil vypnutím predmetného webu, pretože sa jednalo o už nepoužívanú službu. Tu by sme chceli upozorniť na dôležitosť nastavenia správnej politiky manažmentu aktív, ktorej jedným z cieľov je udržiavať prehľad v službách a efektívne aktualizovanie či vypínanie obsolentných služieb.

CSIRT.SK vo februári zaregistroval informáciu o predaji uniknutých dát používateľov parkovacej aplikácie EasyPark, ktorú používajú aj niektoré slovenské mestá. Jednotka informáciu zdieľala s národnou jednotkou SK—CERT NBÚ a agentúrou 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. Systém Achilles slúži tiež na monitoring dostupnosti webových domén.

Mesačník zraniteľností február 2024

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
    - Ubuntu Linux
    - FortiOS, FortiProxy
    - Foxit PDF Reader, Foxit PDF Editor

UPRAV LINK https://www.csirt.gov.sk/aktualne-7d7.html?id=162