ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Jún 2019

Vypracoval: CSIRT.SK

TLP: White

Kybernetické hrozby nemajú dnes len podobu phishingu, malvéru, prienikov do systému, alebo spôsobovania nedostupnosti služieb (DoS). Vďaka technologickému pokroku je možné ovplyvňovať verejnú mienku falošnými informáciami a diskreditovať nepohodlné osoby rozmanitými veľmi efektívnymi spôsobmi.

Vo februárovej mesačnej správe sme priniesli informáciu o softvéri OpenAI, ktorý dokáže pomocou umelej inteligencie rozvinúť ľubovoľnú vetu do dôveryhodne vyzerajúceho, avšak vymysleného článku. Vývojári kvôli obavám z možného zneužitia pre masívnu tvorbu dezinformácií uverejnili len okliešteňú verziu svojho programu.

Zneužitie podobných nástrojov je veľmi reálne, keď si uvedomíme, v akej miere sa dnes šíria falošné správy za účelom ovplyvňovať verejnú mienku. Sociálne siete pravidelne rušia množstvo štátmi sponzorovaných účtov vytvorených za účelom vedenia kampaní šíriacich dezinformácie, väčšinou spájaných s autoritárskymi režimami. Najčastejšie sa skloňujú Irán, Rusko a Čína, no objavujú sa tiež účty z Venezuely, Kosova, Macedónska a Izraela. Bezpečnostná spoločnosť Sophos uverejnila na svojom blogu príbeh Macedónčanky, ktorá písala dezinformačné články pre stránky, ktoré si zarábali online reklamou a návštevníkov získavali manipuláciou s ich emóciami. Spoločnosť Facebook maže okrem účtov aj tisíce falošných stránok a skupín. Pritom vzniká debata ako zamedziť aktivitu týchto tzv. trollov, alebo botov naprogramovaných na rozbúrenie diskusií, a pritom neohroziť proces slobodnej výmeny názorov serióznych účastníkov. Tvorcovia vplyvových kampaní však držia krok s výskumníkmi, ktorí sa snažia tieto kampane odhaľovať a zmierňovať ich vplyv. Napríklad nedávno bola zaznamenaná kampaň, ktorá vydávala staré správy za nové, vďaka čomu nemohli byť označené ako falošné.

V aprílovej mesačnej správe sme zas písali o malvéri, ktorý vyvinuli výskumníci z izraelskej univerzity, a ktorý dokáže v reálnom čase manipulovať medicínske CT 3D snímky. Dokáže na snímku veľmi dôveryhodne pridať onkologický nález, alebo naopak takýto nález odobrať. Úspešnosť medicínskych odborníkov v odhaľovaní softvérových úprav pri vyhodnocovaní snímok bola podstatne nižšia ako 50%, aj v prípade keď vedeli, že časť snímok je falošná.

Pravdepodobne všetci sme sa niekedy zamysleli nad pravosťou fotografie pri správe, ktorá v nás vzbudzovala pocit nedôvery. Šikovný grafik dokáže s Photoshopom divy. Dnes však naše možnosti významne presahujú úpravy fotografií. Dovoľujú nám vytvárať realistické tváre neexistujúcich ľudí, čo napríklad umožní botom na sociálnych sieťach zakladať dôveryhodnejšie účty s falošnými identitami, nakoľko ich profilové fotografie nebudú dohľadateľné na internete. Môžeme vytvárať tiež falošné videá. Prichádza fenomén „deepfake“, ktorý mení naše vnímanie dôveryhodnosti tohoto média.

Na vytvorenie kvalitného deepfake videa bolo potrebné získať veľké množstvo fotografií, alebo niekoľko minút videozáznamu, čo obmedzovalo použitie týchto techník na okruh významných činiteľov s dostatočným mediálnym priestorom. Podvodné videá, nie nevyhnutne počítačom vytvorené, sa objavili už aj v našich zemepisných šírkach, pričom ich obeťou sa napríklad stal prezident Českej republiky Miloš Zeman. Nové technológie dokážu vytvoriť vierohodné videá už s niekoľkými

fotografiami, čo umožňuje útočníkom zamerať sa aj na menej významné osoby. Výskumníci tak napríklad nechali po prvýkrát v histórii prehovoriť Monu Lisu. Deepfake technológie sa začínajú presadzovať aj v komerčnej sfére, kde ich začal využívať priemysel pre dospelých, aj tvorcovia aplikácií ako Deepnude.

Na hrozby, ktoré so sebou deepfake technológie prinášajú, už začínajú reagovať aj politici. Americký kongres sa obáva ich zneužitia pri prezidentských voľbách v roku 2020 a začína rozpravy o úprave zákonov spojených s umiestňovaním falošných informácií a videí na internete. Vznikajú tiež edukačné projekty. Jedným z nich je projekt spoločnosti Google určený na výuku detí ako rozpoznať falošné správy. Podobné projekty začali vznikať aj u nás. Jedným z nich je napríklad zvolsi.info.

Fenomén dezinformácií je dnes široko známym javom. Slovo „hoax“ sa už rozšírilo aj do IT sektoru. Pre zaujímavosť, niektoré antivírové spoločnosti tak začali označovať programy, ktoré sľubujú vyriešenie neexistujúcich systémových problémov, alebo preháňajú ich význam a snažia sa tak z obetí vylákať nemalé peniaze za ich odstránenie.

Pri výbere informácií dnes musíme byť obozretní, či sa jedná o textové správy, alebo videá. Preto vám na internete prajeme šťastnú ruku a bystrý úsudok, aby vás žiaden bot, ani troll nedobehol.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci jún riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Riešil interný únik údajov niekoľkých osôb u jedného konštituenta. Riešil aj situáciu, kedy dochádzalo k prijímaniu registračných e-mailov do systému iného konštituenta, ako mali. Objavil tiež voľne dostupné skeny niekoľkých občianskych preukazov na portáli ulozto.cz, o čom informoval NBÚ. Na tomto portáli objavil aj dokumenty jednej organizácie zo svojej konštituencie.

V rámci proaktívnej činnosti vykonával CSIRT.SK v mesiaci jún retesty protokolov na zariadeniach svojej konštituencie, ak tieto boli vyžiadané, alebo sa vyskytli nezrovnalosti. V niekoľkých prípadoch tiež asistoval pri odstraňovaní objavených zraniteľností.

CSIRT.SK vykonal niekoľko vyžiadaných externých penetračných testov inštitúcií vo svojej konštituencii.

V rámci aktivít zameraných na zvyšovanie odbornej a vedomostnej úrovne tímu sa členovia CSIRT.SK zúčastnili na niekoľkých vzdelávacích a certifikačných podujatiach a konferenciách.

Významné útoky vo svete

GandCrab ransomvér končí. Operátori sa sťahujú, tvrdia, že zarobili viac ako 2 miliardy USD.

Za rok a pol operátori neslávne známeho ransomvéru GandCrab zarobili celkovo pre seba a svojich klientov na výkupnom vyše 2 miliardy USD. Aspoň podľa svojich tvrdení. Osobne si odniesli 150 miliónov, zvyšok pripadol osobám, ktoré si GandCrab objednali ako službu. Operátori sa na kriminálnom fóre rozlúčili so svojimi klientmi a informovali ich, aby ransomvér prestali distribuovať, nakoľko o 20 dní ukončia prevádzku, čo sa aj stalo. Útočníci za týmto malvérom sú však známi rôznymi vtípkami. Preto bezpečnostní výskumníci predpokladajú, že sumy „zárobkov" môžu byť prehnané.

Prienik do systémov American Medical Collection Agency (AMCA) zasiahol 20 miliónov osôb.

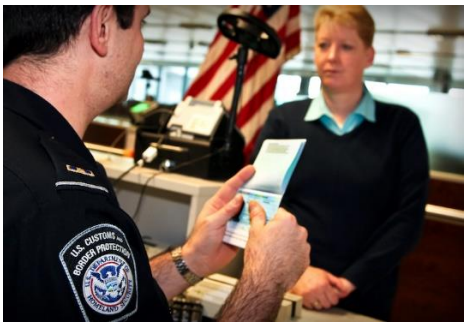
Spoločnosť AMCA utrpela prienik do svojej webovej platobnej stránky. Agentúra vymáha pohľadávky voči svojim klientom, ktorými sú medicínske spoločnosti. Zasiahnutých bolo minimálne 12 miliónov pacientov spoločnosti Quest Diagnostics, 7,7 milióna zákazníkov LabCorp. a 400 000 zákazníkov OPKO Health, troch z klientskych spoločností agentúry. Niekoľko týždňov po ohlásení incidentu podala spoločnosť žiadosť o bankrot.

Čínska univerzita Shanghai Jiao Tong vystavovala 8,4TB Elasticsearch databázu e-mailových metadát voľne do sveta.

Univerzita Shanghai Jiao Tong v Číne vlastnila Elasticsearch databázu, prístup ku ktorej nebol chránený ani heslom. Databáza obsahovala takmer 10 miliárd riadkov, čo predstavovalo približne 8,4TB dát. Tieto obsahovali metadáta množstva e-mailových správ z populárneho open-source e-mailového riešenia

Zimbra. Obsah ani predmet správ nebol prístupný. Univerzita databázu zabezpečila do 24 hodín po nahlásení.

Americkej colnej správe a hraničnej stráži (CBP) unikli fotografie ŠPZ automobilov a tvárí ich majiteľov.



Americká Customs and Border Protection (CBP) oznámila únik fotografií ŠPZ automobilov a tvárí ich majiteľov cestujúcich cez hranice USA, po prieniku do systémov ich dodávateľa, kde boli zálohované. Dodávateľ nebol oprávnený kopírovať tieto dáta do svojej siete, informovala CBP. Organizácia informovala aj policajné zložky a kongres. Dodávateľskou spoločnosťou bola pravdepodobne spoločnosť Perceptics, dodávajúca CBP čítačky ŠPZ automobilov.

Kampaň zneužívajúca zraniteľnosť Exim mailserverov zasahuje 57% mailserverov na svete.

Zraniteľnosť mailserverov bežiacich na platforme Exim, CVE-2019-10149 nazývaná „Return of the WIZard“, bola pod paľbou minimálne dvoch skupín útočníkov. Jedna skupina experimentovala s rôznym typom malvéru, zatiaľ čo druhá vytvárala na zranietľných serveroch zadné vrátka pomocou shell skriptu pridávajúceho SSH kľúč do účtu root. Druhý útok obsahoval aj komponent s vlastnosťami červa, schopný samostatne šíriť malvér na ďalšie Exim serveri, a tiež malvér na ťažbu kryptomien. Zraniteľnosť umožňuje odoslaním e-mailu na server vzdialene vykonávať kód, často s právami root.

Kanadské mesto Burlington prišlo o 500 000 CAD kvôli phishingu.

Kanadské mesto Burlington prišlo o 500 000 CAD po tom, ako zamestnanci magistrátu naleteli phishingovému e-mailu. Pravdepodobne sa jednalo o BEC – business email compromise útok, pri ktorom najprv útočník kompromituje e-mailovú schránku zamestnanca spoločnosti, naštuduje si jej obsah, čím

získa prehľad o aktivitách a partneroch spoločnosti, a nakoniec vytvorí na základe získaných informácií dôveryhodne pôsobiaci phishingový e-mail. Zamestnanci odoslali platbu na cudzí účet v presvedčení, že jeden z dlhodobých dodávateľov mesta zmenil číslo účtu. Phishingový e-mail bol podľa informácií profesionálne vyhotovený aj s doplnkovými dokumentami. Zamestnanci nespozorovali známky podvodu.

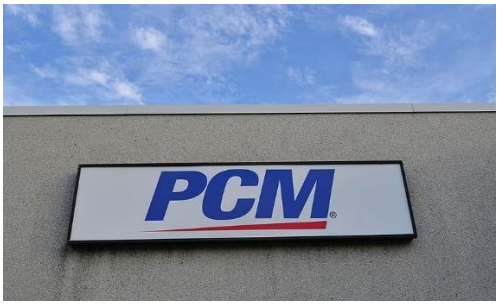
Útoky z iránskej IP adresy na DNA sekvenačné aplikácie dostupné online.

Útočníci operujúci z iránskej IP adresy skenujú internet a hľadajú webové aplikácie dnaLIMS DNA sekvenačných zariadení. Následne zneužívajú 0-day zraniteľnosť, ktorú vývojárska spoločnosť v aplikácii neopravila už dva roky. To umožňuje útočníkom implantovať shell, cez ktorý môžu vzdialene ovládať aplikačný server. Účel útokov zatiaľ nie je jasný, no pravdepodobné sú dve možnosti. Útočníci buď vytvárajú botnet na ťažbu kryptomien, alebo inú podobnú činnosť, alebo sa zaujímajú o DNA dáta, ktoré môžu predať na čiernom trhu, či inak zneužiť.

Celosvetová kampaň čínskych útočníkov voči telekomunikačným operátorom.

Výskumníci spoločnosti Cybereason Nocturnus odhalili niekoľkoročnú celosvetovú kampaň čínskych útočníkov vedenú voči telekomunikačným operátorom. Ohrozené sú používateľské dáta stoviek miliónov používateľov. Útočníci si v sieťach telekomunikačných spoločností vytvorili silnú pozíciu a exfiltrujú veľké množstvá dát v malých dávkach, aby predišli detekcii. Priamo v sieťach spoločností môžu vyhľadávať ľubovoľné záznamy hovorov osôb v ich hľadáčiku. Dokážu si vytvoriť kompletný obraz o osobe a jej živote. Útočníci dokážu tiež zhodiť sieť a spôsobiť tak DoS útok.

Poskytovateľ cloudových služieb PCM pod útokom. Útočníci získali prístup k systémom zdieľania súborov a e-mailovým službám niektorých klientov spoločnosti.



Spoločnosť PCM, jeden z najvýznamnejších poskytovateľ cloudových služieb v USA, utrpel prienik do svojich systémov, ktorý umožnil útočníkom prístup k e-mailovým službám a systémom zdieľania súborov niektorých klientov spoločnosti. Klientela spoločnosti pozostáva z firiem a štátnych aj federálnej vlády. Útočníci získali administratívne prístupy pre manažovanie zákazníckych účtov. Jeden z klientov informoval, že útočníci mali pravdepodobne v úmysle odcudziť informácie zneužiteľné na podvody s darčekovými poukážkami.

Nezabezpečené Amazon S3 úložiská spoločnosti Attunity umožňovali prístup k dátam spoločností Netflix, TD Bank, Ford a ďalších.

ATTUNITY
A Division of Qlik

Spoločnosť Attunity, zaoberajúca sa manažovaním dát, vlastnila tri cloudové úložiská Amazon S3, ktoré neboli zabezpečené a umožňovali verejný prístup k informáciám v nich uloženým. Ohrozených tak bolo vyše 1TB citlivých údajov spoločností zo skupiny Fortune 100, vrátane Netflix, TD Bank a Ford. Dáta okrem iného obsahovali vnútorné obchodné a firemné dokumenty, systémové heslá, údaje o zamestnancoch a zálohy e-mailovej komunikácie. Deň po ohlásení spoločnosť úložiská zabezpečila.

- **Čínska personálna agentúra FMC Consulting vystavovala internetu Elasticsearch klaster so životopismi miliónov osôb; tiež osobné údaje.**
- **Australian National University utrpela prienik. Útočníci získali prístup k 19 ročnému archívu citlivých údajov.**
- **Prístupné osobné údaje vyše 1,6 milióna darcov University of Chicago Medicine kvôli nezabezpečenej Elasticsearch databáze.**
- **Malvér predinštalovaný vo firmvéri štyroch modelov low-endových smartfónov. 20 000 nemeckých používateľov infikovaných.**

- **Pozorovaný nový botnet. GoldBrute útočí na 1,6 milióna Windows zariadení so sprístupneným RDP pripojením pomocou brute-force techník.**

- **Logovací server nemenovanej spoločnosti z Fortune 500 umožňoval prístup k 264GB rozličných citlivých dát.**

- **Španielsko vydalo Číne 94 taiwanských občanov obvinených z telefónnych a internetových podvodov namierených najmä proti čínskym občanom.**

- **Stránka Emuparadise utrpela v apríli 2018 prienik do databázy používateľov. Uniknutú databázu s vyše 1,1 milióna účtov dostal portál haveibeenpwned.com tento mesiac od DeHashed.com.**

- **Ransomvér si nevyberá - útok GlobeImposter 2.0 na charitatívnu organizáciu Auburn Food Bank.**

- **Výrobca dielov pre letectvo ASCO zasiahnutý ransomvérom. Prevádzka v štyroch krajinách prerušená na týždeň.**

- **DDoS útok na servery Telegram Messenger pomocou botnetu znemožnil komunikáciu mnohým používateľom po celom svete.**

- **Americká Securities and Exchange Commission varuje spoločnosti pred používaním nezabezpečených sieťových úložísk NAS a databáz – na základe svojich nálezov.**

- **Útočníci šíria malvér na ťažbu kryptomien pomocou nástrojov, ktoré unikli NSA.**

- **Útočná skupina Xenotime zodpovedná za útoky malvérom Triton v roku 2017 sa zameriava na energetický sektor v USA, Ázii a Pacifickej oblasti.**

- **Americké univerzity Graceland University, Oregon State University a Missouri Southern State University oznámili prienik do svojich systémov spojený s únikom dát.**

- **Dáta z iPhonov a viacerých zariadení Android vyššej triedy je možné vytiahnuť softvérom od izraelskej spoločnosti Cellebrite.**

- **Prienik do databázy charity pre transrodové deti Mermaids UK a zverejnenie vyše 1000 e-mailov a osobných údajov.**

- **Američania vraj implantovali útočný malvér do ruskej elektrickej rozvodnej siete ako odpoveď na ruské kybernetické aktivity proti USA.**

- **Gnosticplayers spôsobil ďalší únik osobných informácií. Obeťou bolo 6 miliónov používateľov služby na objednávanie jedla EatStreet.**

- **Po Sextortion podvodníci útočia na firmy. Vyhrážajú sa, že ich zdiskreditujú masívnou spamovou kampaňou v ich mene.**

- **Podvodné robocalls sa zameriavajú aj na nemocnice. Tisíce hovorov mesačne ohrozujú dostupnosť služieb aj životy pacientov.**

- **Phishing pripravil farnosť Saint Ambrose Catholic Parish takmer o 2 milióny USD.**

- **Nezabezpečená databáza floridskej právnej reklamnej agentúry X Social Media sprístupňovala citlivé údaje spoločnosti a identifikačné údaje vojnových veteránov spolu s ich zraneniami.**

- **Mestská rada Riviera Beach na Floride odhlasovala platbu útočníkom 600 000 USD za obnovenie súborov zašifrovaných ransomvérom. Ďalší necelý milión použije na hardvérovú obnovu svojej infraštruktúry.**

- **Odhadované finančné straty USA spôsobené dátovými prienikmi za posledných 10 rokov dosahujú 1,6 bilióna USD.**

- **MongoDB databáza bez hesla obsahujúca predpisy lieku Vascepa 78 000 pacientov prístupná z internetu.**

- **Zamestnanec kanadskej spoločnosti Desjardins Group poskytol prístup k osobným údajom 2,9 milióna jej členov.**

- **Fórum zaoberajúce sa sociálnym inžinierstvom, Social Engineered, kompromitované. Zverejnené osobné údaje 55 000 členov.**

- **USA spustili kybernetický útok na raketové odpaľovacie zariadenia Iránu po zostrelení amerického špionážneho drona, údajne v medzinárodných vodách. Irán popiera účinnosť.**

- **Ďalšie mesto na Floride, Lake City, zaplatilo výkupné 500 000 USD za svoje ransomvérom zašifrované súbory.**

- **5 miliónov záznamov osobných a zdravotných údajov reklamného portálu pre zdravotné poistenie MedicareSupplement.com voľne dostupných kvôli nezabezpečenej databáze MongoDB.**

Závažné zraniteľnosti bežných softvérových produktov

Zero-day zraniteľnosť RDP na Windows 10 umožňuje prístup ku vzdialenému systému

Novo objavená zero-day zraniteľnosť pripojenia RDP autentifikovaného pomocou NLA umožňuje lokálnemu útočníkovi po krátkom prerušení konektivity získať prístup ku vzdialenému systému. Relácia sa totiž obnoví v nezamknutom stave, aj ak obeť pred odchodom od klientskej stanice vzdialený systém zamkla. Nezáleží ani na tom, či systém využíva viacfaktorovú autentifikáciu, či inú dodatočnú ochranu.

Útočníci dokážu obísť bezpečnostnú kontrolu v macOS Mojave

Operačný systém spoločnosti Apple, MacOS Mojave, obsahuje zraniteľnosti, ktoré umožňujú prostredníctvom malvéru vykonávať syntetické kliknutia a obchádzať tak bezpečnostné prvky systému. Útočník tak môže získať prístup k citlivým údajom pre aplikácie, ktoré si na to musia pýtať povolenie. Môže tiež nainštalovať zraniteľné rozšírenia jadra, ktoré môže zneužiť na ďalšiu fázu útoku a ovládnutie zariadenia.

Závažné zraniteľnosti v Kace K1000

V zariadeniach Kace K1000 sa nachádza niekoľko závažných zraniteľností, ktoré umožňujú autentifikovanému útočníkovi prístup k citlivým údajom z aplikačnej databázy a vykonávať JavaScript kód. Zároveň môže vzdialene aj bez autentifikácie pridať nový administrátorský účet, alebo meniť nastavenia na zraniteľnom zariadení.

Závažné zraniteľnosti rkt Container umožňujú root prístup k systému

Prostredie rkt Container obsahuje závažné zraniteľnosti, ktoré umožňujú kvôli nedostatočnej ochrane vzdialene vykonávať kód a uniknúť z kontajnera. Pri tom môže úspešný útočník získať root práva na hostiteľskom systéme. Opravné aktualizácie nie sú plánované.

TLP: White

Zraniteľnosti v prehrávači VLC Media Player umožňujú prevziať kontrolu nad počítačom

Multimediálny prehrávač VLC Media Player, ktorý používajú stovky miliónov používateľov, mal dve závažné zraniteľnosti, ktoré umožňovali útočníkom vzdialene vykonávať ľubovoľný kód na zraniteľnom systéme a prevziať nad ním úplnú kontrolu. Zraniteľné verzie VLC Player je možné zneužiť pomocou špeciálne upraveného súboru MKV, alebo AVI, ktorý používateľ spustí po stiahnutí, alebo streamuje z internetu.

Zraniteľnosti Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Industrial Network Director (CVE-2019-1861): kvôli nevhodnému vyhodnocovaniu nahraných súborov umožňoval aktualizačný modul programu vzdialene vykonávať kód s právami aplikácie.
Cisco IOS XE (CVE-2019-1904): softvér bol zraniteľný voči CSRF útoku, nakoľko nevhodne vyhodnocoval HTTP požiadavky. Zraniteľnosť sa nachádzala vo webovom manažovacom rozhraní a útočníkom umožňuje vzdialene vykonávať administrátorské zmeny.
Cisco DNA Center (CVE-2019-1848): kvôli nevhodnému obmedzeniu prístupu k systémovým portom bolo možné obchádzať autentifikáciu a získať administrátorské práva. Útočník mohol zapojiť neautorizované zariadenie na podsieť určenú pre klastrové služby.
Cisco Data Center Network Manager (CVE-2019-1620): kvôli nesprávnemu nastaveniu povolení existovalo v manažovacom rozhraní softvéru viacero bezpečnostných zraniteľností. Útočník mohol nahrať do zariadenia špeciálne upravené dáta, čo mu umožnilo zapisovať ľubovoľné súbory a vykonávať kód s právami root.
Cisco TelePresence Endpoint (CVE-2019-1878): kvôli nedostatočnému overeniu prijatých CDP paketov bolo možné po odoslaní špeciálne upravených CDP paketov vykonávať ľubovoľné príkazy v kontexte zraniteľného zariadenia.

Zraniteľnosti VMware

V produktoch VMware bolo opravených viacero rozličných kritických a závažných zraniteľností:
VMware Tools (CVE-2019-5522): chyba čítania mimo povolených hodnôt umožňovala lokálny únik informácií. Zasahuje vm3dmp driver.
VMware Workstation (CVE-2019-5525): zraniteľnosť v Advanced Linux Sound Architecture (ALSA) umožňovala útočníkovi vykonávať ľubovoľný kód na linuxovom hostiteľskom systéme s právami používateľa, pod ktorým aplikácia bežala.

Zraniteľnosti WhatsApp

Kritické zraniteľnosti CVE-2018-6349 a CVE-2018-6350 v mobilnej aplikácii WhatsApp súvisiace s pretečením medzipamäte zásobníka a čítaním mimo povolené hodnoty boli zapríčinené nevhodnou kontrolou veľkosti prijatého paketu a nevhodnou analýzou RTP hlavičiek. Útočníkom umožňovali vykonávanie ľubovoľného kódu v kontexte aplikácie a vyvolanie DoS podmienok.

Mesačník zraniteľností Jún 2019

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 Flash Player, Acrobat a Reader
5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - VLC Media Player

MS Office zneužívaný na šírenie malvéru
macOS Mojave
Kace K1000
rkt Container

https://www.csirt.gov.sk/aktualne-7d7.html?id=196