ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Apríl 2020

Vypracoval: CSIRT.SK

TLP: White

V čase pandémie koronavírusu, ale takisto aj mimo nej, sa v dnešnej dobe často pri téme kybernetickej kriminality objavuje pojem dark web. Metaforicky nazvaný „dark“, v preklade temný, má popisovať jeho činnosť – časť internetu ktorá je zlá, temná, často priamo spojená so závažnými trestnými činmi. Z mnohých činností spájaných s dark webom, ako napríklad nelegálna kúpa a predaj drog, zbraní či iného tovaru ale aj hrozivejších činov ako príprava teroristických útokov sa v dnešnej dobre najviac prejavuje odcudzenie a zverejňovanie osobných údajov.

V súvislosti s COVID-19 sa dark web na istý čas zmenil na zdravotnícky trh. Na jeho stránkach sa predávajú zdravotnícke masky, rúška, rukavice, ale aj lieky či vakcíny proti vírusu. Častými útokmi boli taktiež phishingové emaily, lákajúce používateľov na tému koronavírusu a súčasného stavu vo svete. Podvodné správy ponúkali bezplatné testy, odporúčali vyšetrenia, či mobilné aplikácie. Všetky tieto správy však mali spoločný cieľ – získať od používateľa jeho osobné údaje, prihlasovacie údaje či údaje k bankovým kartám. Útočníci využívajúc (nielen) súčasnú pandémiu sa pomocou phishingových emailov a iných praktík dostávajú k osobným či rôznym prihlasovacím údajom, ktoré následne zverejňujú práve na dark webe s cieľom získania finančnej odmeny, či s iným úmyslom.

Záznamy o používateľoch predávajú na dark webe jednotlivci alebo hackerské skupiny. Príkladom takejto skupiny sú kybernetickí zločinci ShinyHunters, ktorí na dark webe predávajú dáta miliónov používateľov. Zverejňovanie údajov začalo, keď skupina začala predávať dáta viac ako 90 miliónov používateľov, z ktorých väčšina pochádzala z databázy najväčšieho indonézskeho online obchodu Tokopedia. Ďalšími zasiahnutými spoločnosťami boli napríklad online zoznamovacia aplikácia Zoosk, služba Chatbooks či juhokórejská módna platforma SocialShare. Nejaký čas na to skupina ponúkala na predaj databázu s údajmi 22 miliónov používateľov indickej online vzdelávacej platformy Unacademy. To však zločincom stále nestačilo a o pár dní zasiahli znovu – ShinyHunters tvrdili, že sa im podarilo preniknúť na GitHub účet spoločnosti Microsoft a že majú prístup k súkromným adresárom spoločnosti. Z daného účtu údajne následne stiahli 500 GB súkromných projektov a plánovali ich predať, nakoniec sa však rozhodli zverejniť ich zdarma. Hackeri zverejnili ako „ochutnávku“ 1 GB dát pochádzajúcich z údajne odcudzených projektov, avšak po ich preskúmaní spoločnosť usúdila, že sa jedná o podvod a tieto projekty nie sú majetkom Microsoftu. Reakciou na to bolo anonymné vyhlásenie zamestnanca spoločnosti Microsoft, ktorý potvrdil že zverejnené súbory sú pravé, na čo iní zamestnanci zmazali z Twitteru svoje prehlásenia o nepravosti týchto súborov, čím potvrdili odcudzenie projektov z ich GitHub stránky.

Prípady o podobných únikoch sa objavujú aj na platformách zameraných na streamovanie filmov a seriálov. Už hodinu po tom, ako bola koncom roka 2019 spustená video streamingová služba Disney+, hackeri nestrácali čas a na dark webe začali ponúkať odcudzené účty používateľov zadarmo, či za malý poplatok od 3 do 11 dolárov. Tento útok sa uskutočnil len niekoľko hodín po spustení portálu a cena, za ktorú boli účty ponúkané na dark webe, presahovala ich reálnu cenu, ktorú používatelia Disney+ zaplatili za členstvo, čo predstavuje 7 dolárov.

Ďalším príkladom je najpoužívanejšia aplikácia na riešenie matematických problémov Mathway. Útočníkom z už spomínanej skupiny ShinyHunters sa z tejto aplikácie podarilo odcudziť viac ako 25

miliónov emailov a hashovaných hesiel. Tieto údaje boli následné ponúkané na predaj na dark webe za 4000 dolárov v kryptomene Bitcoin, alebo Monero. Algoritmus, ktorý bol použitý na hashovanie hesiel však nebol známy. Keďže údaje nebolo možné použiť na prihlásenie sa do aplikácie, tento artikel nebol lákavou kúpou.

V posledných mesiacoch sa na dark webe okrem odcudzených účtov často objavujú aj rôzne nepravé návody na to, ako spáchať rôzne podvody. Podľa výskumu až 49% dát predaných na dark webe tvoria návody a postupy na to ako napríklad odcudziť emailové účty či prelomiť heslo. Najčastejším cieľom v takýchto návodoch sú okrem konkrétnych organizácií spoločnosti vo finančnom rezorte. Ďalšími „produktami“, ktoré sú na dark webe najčastejšie kupované, sú ukradnuté osobné údaje, účty či údaje k platobným kartám.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci apríl riešil najmä phishingové kampane na svoju konštituenciu. Jednotka riešila tiež niekoľko kompromitácií e-mailových účtov v rámci svojej konštituencie. Okrem toho CSIRT.SK pokračoval v riešení wiper útoku na databázu svojho konštituenta, spojeného s požiadavkou o výkupné za navrátenie zmazaných dát a ich nezverejnenie.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK pokračovala v komunikácii so svojou konštituenciou v rámci odstraňovania zraniteľností zistených pri minulo-mesačnom skene. Taktiež vypracovala preklad a rozposlala bezpečnostné usmernenia organizácie CERT-EU pre prácu zamestnancov z domu, keďže počas koronakrízy vzdialené prístupy zamestnancov z domu predstavovali zvýšené bezpečnostné riziko pre organizácie (nielen) štátnej správy.

Významné útoky vo svete

Bol objavený nový IoT botnet s názvom Dark Nexus

Výskumníci v oblasti kybernetickej bezpečnosti objavili nový IoT botnet, ktorý využíva zariadenia na uskutočnenie útokov typu distribuovaného odmietnutia služby. Tento botnet bol nazvaný dark_nexus a pracuje tak, že využíva útoky hrubou silou proti rôznym zariadeniam, ako sú smerovače, videorekordéry a termálne kamery na to, aby ich pripojil do siete botov. V súčasnosti je napadnutých najmenej 1300 zariadení z rôznych krajín, ako napríklad Čína, Južná Kórea, Thajsko, Brazília a Rusko. Bol pravdepodobne inšpirovaný botnetmi Qbot a Mirai, avšak jeho moduly sú poväčšine originálne. Je vytvorený pre 12 rôznych procesorových architektúr a dynamicky sa dodáva na základe architektúry zariadenia.

Čínske vládne VPN servery boli cieľom "zero-day" útoku

Čínska spoločnosť Qihoo 360, ktorá sa venuje kybernetickej bezpečnosti ohlásila, že útočníci z APT skupiny DarkHotel využili zero-day zraniteľnosť na útok proti čínskej vládnej VPN službe. Útoky na poskytovateľa VPN SangFor začali v marci a odvtedy bolo napadnutých minimálne 200 VPN serverov. Táto chyba zabezpečenia existovala v procese aktualizácie systému, ktorý sa spustí automaticky, keď sa klient VPN začne pripájať k serveru. Klient získava aktualizáciu z konfiguračného súboru uloženom na pevnom mieste na pripojenom VPN serveri a stiahne si program s názvom SangforUD.exe. Pred tým sa však nevykonávajú žiadne bezpečnostné kontroly a preto je možné zmeniť konfiguračný súbor a nahradiť aktualizačný program vlastným škodlivým kódom.

Údaje 4 miliónov používateľov Quidd boli nájdené na dark webe

Súbor údajov obsahujúci 3,954,416 používateľských údajov bol nájdený na hackerskom fóre na dark webe. Spoločnosť Quidd ponúka aplikáciu na obchodovanie s digitálnymi zberateľskými predmetmi. V týchto dátach sa nachádzali emailové adresy, používateľské mená, a hashované heslá. Taktiež tam bolo objavených vyše tisíc pracovných emailov. Týkajú sa subjektov AIG, Experian, Target, Microsoft, Accenture, Virgin media a iných.

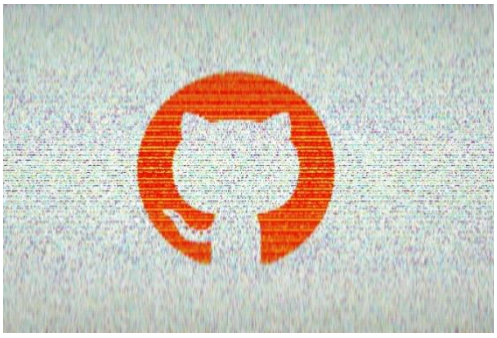
Za útokom na letisko v San Franciscu stoja ruskí hackeri

Hackeri, o ktorých sa predpokladá, že pôsobia v mene ruskej vlády napadli dve webové stránky prevádzkované medzinárodným letiskom v San Franciscu. Podľa predstaviteľov letiska, útočníci na obe stránky nasadili škodlivý kód, ktorý využíval zraniteľnosť v prehliadači Internet Explorer. Tým sa pokúšali kradnúť prihlasovacie údaje. Spoločnosť ESET tvrdí, že že zámerom bolo zhromaždiť Windowsové prihlasovacie údaje (používateľské meno a NTLM hash) návštevníkov. Využívali vlastnosti protokolu SMB. Podľa ESETu bol tento útok vykonaný skupinou útočníkov s prezývkou Energetic Bear, ktorá pravdepodobne pôsobí v Rusku.

Heslá aplikácie Zoom sú na predaj na Dark Webe

Na hackerských fórach a na dark webe je na predaj viac ako 500 tisíc účtov aplikácie Zoom za menej ako cent, v niektorých prípadoch sa rozdávajú zadarmo. Tieto údaje boli zhromažďované prostredníctvom útokov hrubou silou, pri ktorých sa útočníci pokúšali prihlásiť do aplikácia Zoom pomocou údajov zo starších únikov. Údaje, pomocou ktorých sa podarilo úspešne prihlásiť, boli pridané do zoznamov, ktoré sa predávali iným hackerom. Okrem emailovej adresy a hesla obete obsahujú aj URL súkromnej miestnosti používateľa a jeho HostKey.

Prihlasovacie údaje do GitHubu boli ukradnuté pomocou phishingu



Na používateľov GitHubu bola zacielená phishingová kampaň, ktorá bola vytvorená na zhromažďovanie a odcudzenie prihlasovacích údajov pomocou webstránky, ktorá napodobňovala úvodnú prihlasovaciu stránku. Okrem kradnutia prihlasovacích údajov, útočníci automaticky sťahujú obsah súkromných repozitárov, vrátane účtov organizácie a jej spolupracovníkov. Po úspešnom získaní prihlasovacích údajov môže útočník autorizovať OAuth aplikáciu na účte s cieľom zachovania prístupu v prípade, že si používateľ zmení svoje heslo.

Spoločnosť Nintendo potvrdila únik prihlasovacích údajov až 160 tisíc účtov

Po tom, čo používatelia ohlásili neoprávnené prihlásenia a nákupy z ich účtov, spoločnosť Nintendo potvrdila, že viac ako 160 tisíc účtov bolo napadnutých v dôsledku zneužitia pôvodného prihlasovacieho systému. Uviedli, že útočníci od začiatku apríla zneužívajú NNID (Nintendo Network ID) prihlasovací systém, aby prenikli do užívateľských účtov. NNID sa primárne používal pre Nintendo 3DS a konzolu Wii U. NNID je možné prepojiť s účtom Nintendo a použiť ho ako možnosť prihlásenia. Tým môže útočník získať prístup k platobným údajom (PayPal alebo platobné karty), ktoré sú potrebné na nákupy v hrách.

Útočník zverejnil 23 miliónov používateľských mien a hesiel z detskej hry Webkinz

Útočník zverejnil používateľské mená a heslá takmer 23 miliónov hráčov Webkinz World, online hry pre deti, ktorá je spravovaná kanadskou spoločnosťou Ganz. Spoločnosť ZDnet získala kópiu uniknutého súboru pomocou služby na monitorovanie únikov dát s názvom „Under the Breach“. Tento súbor s veľkosťou 1GB obsahoval 22 982 319 párov používateľských mien a hesiel, pričom heslá boli hashované pomocou algoritmu MD5. Útočník údajne získal prístup do databázy pomocou SQL injection útoku na zraniteľnosť nachádzajúcu sa v jednom z formulárov webovej stránky.

Hackerské fórum bolo napadnuté a bola zverejnená databáza OGUsers

Konkurenční hackeri znova zaútočili na OGUsers, fórum, ktoré sa venuje obchodovaniu s ukradnutými účtami z Instagramu, Twiteru a s kradnutými bitcoin účtami. Zverejnili databázu s približne 200 000 užívateľskými záznamami. Heslá užívateľov pravdepodobne neboli šifrované, pretože viac ako polovica z nich bola zverejnená v plaintexte.

Zbierka platobných kariet z Južnej Kórei a USA sa objavila na dark webe

Na dark webe sa objavila zbierka približne 400 000 záznamov o platobných kartách, hlavne z Južnej Kórei a Spojených štátov. Celková cena tejto databázy je skoro 2 milióny dolárov, čo predstavuje asi 5 dolárov za záznam. Obsahuje najmä identifikačné číslo banky (BIN), číslo účtu, dátum vypršania platnosti a overovacie číslo (CVV). Takéto údaje sa získavajú z infikovaných POS terminálov, bankomatov alebo zraniteľných platobných systémov.

Na dark webe je na predaj 600 000 používateľských údajov, ktoré unikli poskytovateľovi emailových služieb

email.it

Taliansky poskytovateľ emailových služieb Email.it potvrdil, že boli obeťou kybernetického útoku. Útočníci zo skupiny NN (No Name) tvrdia, že k útoku došlo pred viac ako dvoma rokmi, a to v januári 2018. Podľa ich slov vtedy požiadali o malé výkupné a dali im šancu opraviť zraniteľnosti nachádzajúce sa na ich serveroch. Poskytovateľ s nimi však odmietol komunikovať a neupovedomil svojich používateľov o tomto úniku. Uniknuté databázy by mali obsahovať nešifrované heslá, bezpečnostné otázky, obsahy emailov a ich prílohy.

267 miliónov profilov Facebooku sa predalo za 600 dolárov

facebook

Útočníci predávajú na dark webe a na kybernetických kriminálnych fórach viac ako 267 miliónov profilov Facebook za 500 libier. Aj keď žiadny z týchto záznamov neobsahuje heslá, obsahuje informácie, ktoré by útočníkom uľahčili vykonávanie phishingových útokov na kradnutie prihlasovacích údajov. Mnohé z týchto záznamov obsahovali celé meno používateľa, telefónne číslo a jedinečné ID.

TLP: White

- Malvér s názvom AnarchyGrabber kradne účty z chatovacej aplikácie Discord.
- Útočníci ukradli z platformy Lendf.me kryptomenu v hodnote 25 miliónov dolárov
- Vírus Emotet narušil chod siete v organizácii prehriatím všetkých počítačov.
- Nemecká vláda mohla pri phishingových útokoch ohľadom COVID-19 stratiť desiatky miliónov eur
- Aplikácii digitálnej peňaženky Key Ring unikli informácie milióna používateľov
- Bola zverejnená databáza RigUp obsahujúca 76 000 súborov z amerického energetického sektora
- Nová kampaň malvéru Kinsing bola cielená na nástroj Docker.
- Čínska kybernetická úťočná skupina Winnti sa zamerala na hernú spoločnosť
- SBA odhalila potenciálny únik údajov, ktorý má vplyv na 8 000 žiadateľov o núdzové obchodné pôžičky
- Spear-phishing kampaň využíva COVID-19 na šírenie trójskeho koňa Lokibot, ktorý je určený na kradnutie informácií.
- Spoločnosť Chegg poslala svojim zamestnancom oznámenie, v ktorom ich informovala o úniku údajov, ku ktorému došlo začiatkom tohto mesiaca.
- Kybernetický zločinec použil ukradnuté prihlasovacie údaje do služby Active Directory na vydieranie nemocníc v Spojených štátoch amerických
- Stránke venujúcej sa GDPR unili data a heslá
- USA ponúka 5 miliónov dolárov za informácie o severokórejských útočníkoch
- Ransomvér Clop zverejnil súbory americkej farmaceutickej spoločnosti ExecuPharm po tom, čo rokovania o výkupnom údajne zlyhali.

- **Útočníci „PerSwaysion“ zneužili aplikáciu Microsoft Sway vo phishingovom útoku zameranom na vedúcich pracovníkov spoločnosti.**

- **Nový Android malvér „EventBot“ zneužíva prístupové funkcie na odfiltrovanie citlivých údajov z finančných aplikácií, na čítanie správ používateľov a na odcudzenie SMS autentifikačných kódov.**

- **Milióny útokov hrubou silou útočia na účty vzdialenej pracovnej plochy (RDP), cieľom je prevziať podnikové počítače a preniknúť do sietí.**

- **Útočníci sponzorovaní štátom využili zero-day zraniteľnosť u estónskeho poskytovateľa e-mailových služieb Mail.ee, aby sa dostali k e-mailovým účtom vysoko postavených používateľov.**

- **Prebiehajúca špionážna kampaň šírená prostredníctvom Google Play zameraná na používateľov Androidu v Ázii je pravdepodobne dielom OceanLotus APT actora-a.**

- **Izraelská vláda tvrdí, že hackeri sa minulý týždeň zamerali na spoločnosti venujúce sa dodávke a úprave vody a prikázala im, aby zmenili heslá.**

- **Bolo odhalených viac ako 150 000 e-mailov, ktoré šíria trójskeho koňa pre vzdialený prístup (RAT), používajúc randenie pre dospelých ako návnadu, pričom takmer polovica z nich bola odoslaná na e-mailové adresy univerzít v USA.**

- **Prevádzkovatelia ransomvéru Shade (Troldesh) skončili svoju činnosť a ako prejav dobrej vôle vydali viac ako 750 000 dešifrovacích kľúčov, ktoré môžu obete použiť na získanie prístupu ku svojim súborom.**

- **Nová phishingová kampaň šíri backdoor malvér od vývojárov TrickBot-u, ktorý útočníci používajú na získanie úplného prístupu k podnikovým sieťam.**

- **Útočníci zneužívajú čakanie firiem v USA na správy o ich predložených pôžičkách na ochranu miezd, posielajú phishingové e-maily zamerané na získanie prihlasovacích údajov.**

- **Znaky v sindhskom jazyku môžu pokaziť telefóny iPhone a ďalšie zariadenia so systémom iOS / macOS, ak si obeť otvorí texty, príspevky na Twitteri alebo správy v rôznych aplikáciách, ktoré ich obsahujú.**

TLP: White

- Pri neoprávnenom získavaní údajov sa na odcudzenie prihlasovacích údajov používajú upozornenia na stretnutie Zoom.

- Právny spor medzi Facebookom a izraelským dodávateľom spyware NSO Group: Stovky útokov WhatsApp sú spojené s jedinou IP adresou.

- ESET dokázal zničiť niekoľko C&C serverov botnetu „VictoryGate“, ktorý sa šíri infikovanými zariadeniami USB, čím narušil jeho činnosť.

- Podvodníci posielajú e-maily, ktoré sa vydávajú za federálny rezervný systém USA a lákajú príjemcov na finančné úľavy prostredníctvom programu na ochranu platieb.

- NSA súbory, ktoré zverejnila skupina Shadow Brokers, poukazujú na neznámu APT skupinu.

- Kriminálnici použili údaje, ktoré údajne ukradli WHO, CDC a ďalším významným skupinám, na šírenie dezinformácií o koronavíruse.

- Útočníkom sa podarilo oklamať tri britské spoločnosti, aby previedli celkom 1,3 milióna dolárov na ich bankové účty, zatiaľ čo vedúci pracovníci si mysleli, že uzavreli investičnú dohodu so startupmi.

- Zdrojový kód Team Fortress 2 a Counter-Strike: Global Offensive od Valve bol zverejnený na internete na stiahnutie pre kohokoľvek .

- Skupina šíriaca škodlivé reklamy Tag Barnakle sa dostala do reklamných serverov Revive a neopatrným návštevníkom ponúka škodlivé reklamy.

- Čínska hackerská skupina Evil Eye využíva novú techniku útoku v zariadeniach iOS na inštaláciu spywaru zameraného na moslimskú menšinu Uyghur.

- Mesto Torrance v Los Angeles bolo údajne napadnuté DoppelPaymer ransomvérom, boli ukradnuté nezašifrované údaje a zašifrované zariadenia.

- Bitdefender tvrdí, že cieľom nedávnych útokov využívajúcich spyware „Agent Tesla“ boli organizácie na ťažbu ropy a zemného plynu.

- **Cognizant, gigant služieb informačných technológií, bol cieľom kybernetického útoku, údajne pochádzajúceho od prevádzkovateľov ransomvéru Maze.**

- **Podvodný malvér požadajúci výkupné vydiera používateľov zverejnením nahrávky na ktorej sú údajne oni sami.**

- **Hackeri zameriavajúci sa na Azerbajdžan, prejavili záujem o energetický sektor, konkrétne o systémy SCADA týkajúce sa veterných turbín.**

- **Technická spoločnosť Wappalyzer zverejnila bezpečnostný incident, po tom ako útočník začal posielať ich zákazníkom ponuku na predaj ich databázy za 2 000 dolárov.**

- **Falošné rozšírenia v prehľadávači sa maskovali ako legitímne nástroje na kryptomenu.**

- **Webové stránky WordPress WooCommerce boli terčom útokov pomocou zmeny ich JavaScript súborov.**

- **Útočníci používajúci ransomvér Ragnar Locker zašifrovali systémy portugalského energetického gigantu Energias de Portugal (EDP) a teraz žiadajú výkupné za 1580 BTC (10,9 milióna dolárov).**

- **Distribútor škodlivého softvéru uzamkol počítače obetí skôr, ako mohli spustiť systém Windows, následne z toho obvinil dvoch uznávaných výskumných pracovníkov v oblasti bezpečnosti.**

- **Nový výskum použil technológiu 3D tlače na obídenie snímačov odtlačkov prstov, výsledky boli otestované na mobilných zariadeniach Apple, Samsung a Microsoft.**

- **Travelex údajne zaplatil výkupné vo výške 2,3 milióna dolárov, aby dostal svoje systémy späť online po zašifrovaní ransomvérom Sodinokibi.**

- **Hammersmith Medicines Research, výskumná spoločnosť testujúca vakcíny proti koronavírusu, rozposielala výstrahy po ransomvérovom útoku.**

- **Austrálčania, ktorých finančne postihla pandémia COVID-19, sa stávajú terčmi podvodníkov, ktorí sa od polovice apríla pokúšajú dostať do rúk čiastočne uvoľnené finančné prostriedky obetí.**

- **Malvér LimeRAT sa šíri technikou šifrovania VelvetSweatshop v nástroji Excel.**

- **Prevádzka určená pre viac ako 200 najväčších sietí na dodávanie obsahu (CDN) a poskytovateľov cloudhostingu na svete, bola podozrivo presmerovávaná cez ruského telekomunikačného poskytovateľa Rostelecom.**

- **Igor Golovin, analytik v spoločnosti Kaspersky, konečne odhalil, ako sa malvér xHelper Android preinštalováva aj po obnovení továrenských nastavení.**

- **Twitter informoval používateľov o tom, že ich osobné údaje mohli byť odhalené v dôsledku spôsobu, akým webový prehliadač Firefox ukladá údaje v pamäti.**

- **Nedávno odhalená kampaň, ktorá bola sledovaná od mája 2018 sa zameriavala na Microsoft SQL servery pomocou malvérov vytvárajúcich zadné vrátka.**

- **Útočník prenikol na servery Elasticsearch a pokúsil sa vymazať ich obsah, vinu sa snažil hodiť na spoločnosť pôsobiacu v oblasti kybernetickej bezpečnosti.**

- **Nový útok používa ochrannú známku Svetovej zdravotníckej organizácie, aby prilákal používateľov informáciami o koronavíruse.**

Závažné zraniteľnosti bežných softvérových produktov

Zero-day zraniteľnosť aplikácie Zoom pre Windows umožňuje šírenie malvéru a vykonávanie kódu

V aplikácii Zoom zameriavajúcej sa na video konferenčné hovory bola nájdená kritická zero-day zraniteľnosť. Nachádza sa v klientovi aplikácie na operačnom systéme Windows. Táto zraniteľnosť vzniká v spôsobe akým aplikácia spracováva Uniform Resource Identifier (URI) cesty a jej zneužitie umožňuje útočníkovi vzdialené vykonávanie kódu. Po zneužití zraniteľnosti môže útočník získať informácie o sieti alebo tiež vykonať útok UNC injection (Universal Naming Convention).

Cisco opravilo kritické zraniteľnosti vo viacerých produktoch

Spoločnosť Cisco vydala bezpečnostné záplaty na kritické a závažné zraniteľnosti viacerých produktov. Vzdialený útočník mohol tieto zraniteľnosti využiť so zámerom získať kontrolu nad postihnutým systémom, vykonávať kód, či spôsobiť nedostupnosť služby. Americká vládna agentúra CISA nabáda užívateľov a administrátorov, aby zraniteľné systémy bezodkladne aktualizovali.

VMWare opravil kritickú zraniteľnosť vo vCenter Server a dve závažné vo vRealize Log Insight

Spoločnosť VMWare opravila kritickú zraniteľnosť v produkte vCenter Server, ktorá umožňovala útočníkom získať citlivé informácie zo služby Directory Service, s ktorých pomocou mohli prevziať kontrolu nad celou infraštruktúrou. Opravené boli aj dve zraniteľnosti v produkte vRealize Log Insight, ktoré kvôli nevhodnej kontrole vstupov umožňovali ovládnutie zraniteľných zariadení.

Na platforme Git bola odstránená kritická zraniteľnosť

Vytvorením špeciálne upravenej adresy URL, ktorá obsahuje zakódovaný nový riadok, môžu byť do toku paketov vložené neočakávané hodnoty. Útočník tak môže pomocou špeciálne vytvorenej adresy URL docieliť, že klient Git vloží prihlasovacie údaje svojho hostiteľského serveru do HTTP požiadavky pre ľubovoľný cudzí server.

TLP: White

Štyri zero-day zraniteľnosti produktu IBM Data Risk Manager boli zverejnené online

Na portáli Github boli zverejnené štyri kritické zraniteľnosti produktu IBM Data Risk Manager v kategóriách obídenie autentifikácie, vkladanie príkazov, nezabezpečené predvolené heslo a ľubovoľné sťahovanie súborov. Útočník ich zneužitím môže vzdialene vykonávať kód, sťahovať zo systému ľubovoľné súbory či ovládnuť zraniteľnú infraštruktúru.

V knižnici Autodesk FBX boli opravené závažné zraniteľnosti

Spoločnosť Autodesk zverejnila opravy na bezpečnostné chyby nájdené v knižnici Autodesk FBX-SDK, ktorú využíva viacero systémov pre spracovanie 3D obsahu. Úspešné zneužitie zraniteľnosti umožňuje získanie kontroly nad cieľovým zariadením, vzdialené vykonanie ľubovoľného kódu alebo odmietnutie služby (DoS).

Chyba OpenSSL umožňuje spôsobiť nedostupnosť služby

Nesprávne narábanie s rozšírením TLS 1.3 „signature_algorithms_cert“ vedie pri nadväzovaní spojenia medzi serverom a klientom a volaní funkcie SSL_check_chain() ku zlyhaniu aplikácie, čo má za následok vyvolanie nedostupnosti služby. Verzie OpenSSL 1.1.1d, 1.1.1e a 1.1.1f sú postihnuté chybou, ktorú je možné zneužiť na útok typu DoS.

Obídenie autentifikácie vo FortiMail a FortiVoiceEnterprise

Zraniteľnosť vo FortiMail a FortiVoiceEnterprise s označením CVE-2020-9294 umožňuje vzdialenému útočníkovi obídenie autentifikácie a získanie prístupu do systému ako oprávnený užívateľ. Zraniteľnosť sa nachádza v službe pre obnovenie hesla a umožňuje neoverenému útočníkovi na diaľku požiadať o zmenu hesla a tým získať prístup k účtom iných používateľov.

Foxit Reader, PhantomPDF a doplnok U3DBrowser obsahujú závažné bezpečnostné zraniteľnosti

Spoločnosť Foxit Software vydala záplaty závažných bezpečnostných zraniteľností pre jej platformy na čítanie a editáciu PDF. Niektoré z chýb umožňujú vzdialenému útočníkovi vykonať v zraniteľných systémoch ľubovoľný kód.

Zraniteľnosti VMware

V produktoch VMWare bolo opravených viacero rozličných kritických a závažných zraniteľností:
CVE-2020-3953 CVE-2020-3954: Kvôli nesprávnemu ošetrovaniu kódu vloženého užívateľom je spôsobená zraniteľnosť vloženia HTML vykonateľného kódu od ľubovoľného používateľa. Zneužitie týchto zraniteľností môže útočníkovi umožniť prebratie kontroly nad počítačom obete.
CVE-2020-5406: Zraniteľnosť nastáva v aplikácii VMWare Tanzu, ktorá si ukladá prihlasovacie údaje do databázy.

Zraniteľnosti Intel

V produktoch Intel neboli opravené žiadne kritické ani závažné zraniteľnosti.

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Unified Communications Manager CVE-2020-3177: Aplikácia je náchylná na kritickú zraniteľnosť adresára kvôli nedostatočnej validácii vstupu dodávaného používateľom do rozhrania postihnutého zariadenia.
Multiple Cisco IP Phones CVE-2020-3161: Viacero telefónov Cisco IP je náchylných na umožnenie vzdialeného vykonávania kódu pomocou špeciálne vytvorených HTTP požiadaviek. Úspešné zneužitie zraniteľnosti útočníkovi umožňuje vykonať ľubovoľný kód s oprávneniami administrátorského používateľa root.

Cisco IoT Field Network Director CVE-2020-3162: Softvérová platforma IoT Field Network Director v dôsledku nesprávneho vyhodnocovania vstupov umožňuje vznik zraniteľnosti spôsobujúcej odmietnutie služby.
Cisco Wireless LAN Controller CVE-2020-3273: Bezdrôtový ovládač Cisco umožňuje vznik zraniteľnosti spôsobujúcej odmietnutie služby kvôli zlyhaniu pri overovaní totožnosti vstupu dodávaného používateľom do funkcie 802.11 Generic Advertisement Service (GAS).
Cisco Aironet Series Access Points CVE-2020-3260: Prístupové body Cisco sú v dôsledku nesprávneho spracovania klientskych paketov odosielaných na ovplyvnené prístupové miesto náchylné na vznik zraniteľnosti spôsobujúcej odmietnutie služby.

Mesačník zraniteľností Apríl 2020

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
   - Zero-day zraniteľnosť aplikácie Zoom pre Windows
   - Cisco opravilo kritické zraniteľnosti vo viacerých produktoch
   - Závažné zraniteľnosti produktov Intel
   - VMWare opravil kritickú zraniteľnosť vo VCenter Server a dve závažné vo vRealize Log Insight
   - Na platforme Git bola odstránená kritická zraniteľnosť
   - Štyri zero-day zraniteľnosti produktu IBM Data Risk Manager boli zverejnené online
   - V knižnici Autodesk FBX boli opravené závažné zraniteľnosti
   - Chyba OpenSSL umožňuje spôsobiť nedostupnosť služby
   - Obídenie autentifikácie vo FortiMail a FortiVoiceEnterprise
   - Foxit Reader, PhantomPDF a doplnok U3DBrowser obsahujú závažné bezpečnostné zraniteľnosti

https://www.csirt.gov.sk/aktualne-7d7.html?id=214