MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

November 2020

Vypracoval: CSIRT.SK

TLP: White

V mesiaci november bola veľmi rozšírenou témou vakcína proti vírusu COVID-19. V období, kedy sa svetové organizácie rozhodli spojiť sily a vytvoriť vakcínu proti koronavírusu sa útočníci chopili šance, a začali na tieto inštitúcie útočiť. Účelom bol pravdepodobne finančný zisk. Vzhľadom k tomu, že svet bojuje s pandémiou, ktorú je nevyhnutné spomaliť, v najlepšom prípade ukončiť, je dôležité zlepšiť bezpečnosť organizácií, ktoré stoja za výskumom vakcíny, farmaceutických spoločností a ďalších príbuzných inštitúcií.

Spoločnosť Microsoft uviedla, že tento mesiac odhalila tri štátom podporované APT skupiny, ktoré podnikali útoky na aspoň sedem významných spoločností zapojených do výskumu ohľadom vakcíny proti COVID-19. Vo všeobecnosti boli útoky zamerané na výrobcov vakcín, výskum a na spoločnosť, ktorá vyvinula test na COVID-19.

Prvou skupinou je skupina ruských útočníkov nazývaná Strontium/Fancy Bear/Sofacy (APT28), ktorá získava prihlasovacie údaje hrubou silou a následne preniká do účtov a kradne citlivé dáta. Ďalšie dve skupiny sú zo Severnej Kórey, pričom prvá z nich je známa pod názvom Zinc alebo Lazarus Group. Táto skupina sa primárne spolieha na phishingové emailové kampane, v rámci ktorých posiela správy s vykonštruovanými popismi pracovných pozícií a vydáva sa za náborových pracovníkov. Druhá skupina zo Severnej Kórey je známa ako Cerium. Vo phishingovej kampani sa vydáva za zástupcov Svetovej zdravotníckej organizácie (WHO) a využíva témy súvisiace s COVID-19. Hackerské skupiny využívajú súčasnú pandémiu vo svoj prospech, a preto sa zamerali práve na organizácie, ktoré pomáhajú v boji proti nej.

Dokonca už v júli americká vláda uviedla, že na výrobcov vakcín sa zameriavali čínski hackeri, na ktorých podali trestné oznámenie. Spoločnosť Microsoft tiež informovala, že väčšina cieľov nachádzajúcich sa v Kanade, Francúzsku, Indii, Južnej Kórei a USA bolo priamo zapojených do výskumu vakcín a liečby COVID-19, pričom vakcíny boli v rôznych fázach klinických štúdií.

Jednou zo zasiahnutých je spoločnosť Americold, ktorá poskytuje chladiarenské skladovacie kapacity pre potravinárske spoločnosti. Práve táto spoločnosť rokovala o poskytnutí skladovania a prepravy teplotne citlivých vakcín proti COVID-19. Útok ransomvérom na Americold tak mohol tiež súvisieť s jej dôležitým postavením v boji s pandémiou. Podľa správ na Twitteri boli napadnuté telefónne systémy spoločnosti, email, správa zásob a plnenie objednávok.

Zasiahnutou bola aj biotechnologická firma Miltenyi, ktorá dodáva kľúčové komponenty potrebné pre výskum liečby COVID-19. Spoločnosť v súčasnosti dodáva antigény SARS-CoV-2 pre výskumníkov pracujúcich na lieku proti koronavírusu. Povaha škodlivého softvéru nie je známa. Aj tento incident môžeme zaradiť do série útokov na spoločnosti pracujúce na výskume a výrobe vakcíny.

V predošlom mesiaci bol zasiahnutý dodávateľ Reddy's Laboratories ruskej vakcíny „Sputnik V". Po kybernetickom útoku odstavil svoje závody v Brazílii, Indii, Rusku, Veľkej Británii a USA. Výrobca liečiv

musel izolovať všetky služby dátového centra, aby mohol obnoviť svoje systémy. Spoločnosť nezverejnila podrobnosti útoku a nevyjadrila sa ani k odpájaniu zariadení.

Vo všeobecnosti sú kybernetické útoky na výskumnícke organizácie v odvetví zdravotníctva globálnym problémom. Na spoločnosti a organizácie venujúce sa výskumu alebo liečbe COVID-19 sa zameriavajú nie len štátom sponzorované APT skupiny, ale aj menšie zločinecké skupiny z rôznych, nie len finančných, dôvodov.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci november riešil štandardne najmä phishingové kampane na svoju konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov.

Okrem toho vládna jednotka preverovala niekoľko zraniteľností v systémoch svojej konštituencie, ktoré nahlásili nemenovaní bezpečnostní výskumníci. Dotknuté subjekty boli po potvrdení zraniteľností kontaktované a boli im odporučené kroky pre ich odstránenie. Jednotka tiež sledovala situáciu ohľadom narastajúcej podvodnej telefonickej kampane, v ktorej sa zahraniční podvodníci vydávajú za technickú podporu Microsoftu, alebo inej všeobecne známej technologickej firmy a obetiam tvrdia, že ich zariadenia majú zraniteľnosť, alebo boli napadnuté hackermi. Situáciu konzultovala s policajnými zložkami, varovala svoju konštituenciu a vydala varovanie na svojom webe.

Jednotka CSIRT.SK v novembri v rámci svojej proaktívnej činnosti začala so spracovaním úniku z portálu Cit0day, v ktorom sa nachádzali prihlasovacie údaje z ukradnutých databáz 23 000 webových stránok. Spolu sa únik dotkol až 226 miliónov používateľov. CSIRT.SK vyselektoval slovenských používateľov a kontaktoval organizácie svojej konštituencie, ktorých účty boli v úniku objavené. O zvyšných nálezoch informoval národnú jednotku SK-CERT pod NBÚ. Okrem toho prebehlo niekoľko testov zraniteľností webových služieb a analýza malvéru z phishingových emailov kampane „ŽIADOSŤ O CENOVÚ PONUKU (Univerzita Komenského v Bratislave)“. Indikátory kompromitácie rozposlala jednotka svojej konštituencii.

CSIRT.SK tento mesiac pokračoval v testovaní bezpečnosti a odhaľovaní zraniteľností v informačných systémoch zdravotníckych zariadení SR dostupných z internetu. Svojou aktivitou jednotka prispela ku zachovaniu ich plnej funkčnosti, ktorá je aj kvôli súčasnej epidemiologickej situácii zásadná.

Významné útoky vo svete

Útočník prezradil údaje o takmer 50 tisíc zraniteľných Fortinet VPN sieťach.

Útočník zverejnil zoznam jednoriadkových foriem zneužitia zraniteľnosti CVE-2018-13379 na odcudzenie prihlasovacích údajov do VPN. Tiež prezradil údaje o takmer 50 tisíc zraniteľných sieťach Fortinet VPN. Na zozname zraniteľných cieľov sú prítomné IP adresy patriace bankám, telekomunikáciám a vládnym organizáciám z celého sveta. Analytik zo spoločnosti Bank_Security tiež našiel na fóre ďalší príspevok, kde boli zdieľané dáta zo súborov „sslvpn_websession“ pre každú IP adresu používateľov pripojených k týmto VPN. Uniknuté súbory obsahujú mená, heslá a demaskované IP adresy. Veľkosť archívu s týmito súbormi je iba 36MB, avšak po dekompresii má viac ako 7GB. Ďalším uniknutým archívom je súbor, ktorý oddeľuje pakistanské VPN IP adresy a korešpondujúce súbory „sslvpn_websession“ od ostatných údajov.

Poskytovateľ zdravotnej starostlivosti AspenPointe utrpel únik údajov o viac ako 295 tisíc pacientoch

Americký poskytovateľ zdravotnej starostlivosti AspenPointe utrpel útok, pričom zasiahnutých bolo viac ako 295 tisíc pacientov. Došlo k neoprávnenému prístupu do siete a útočníci ukradli chránené informácie o zdraví (PHI) a osobné identifikačné údaje (PII). Uniknuté dáta zahŕňajú celé meno a jedno alebo viac z údajov ako dátum narodenia, rodné číslo, Medicaid identifikátor, dátum poslednej návštevy (ak existuje), dátum prijatia, prepustenia alebo diagnostický kód. Organizácia tvrdí, že neexistujú dôkazy o tom, že by tieto odcudzené údaje boli použité tretími stranami.

Únikom údajov spoločnosti Capcom je zasiahnutých viac ako 350 tisíc ľudí

Útočníci pomocou ransomvéru Ragnar Locker ukradli a zverejnili citlivé informácie o zákazníkoch a zamestnancoch spoločnosti Capcom. Capcom je

spoločnosť, ktorá stojí za vývojom hier ako „Street Fighter“, „Resident Evil“, „Ghosts and Goblins“ a podobne. Spoločnosť Capcom zdôrazňuje, že nedošlo k úniku údajov o kreditných kartách, pretože sú spravované externou firmou. Podľa spoločnosti medzi ukradnuté údaje môžu patriť mená, adresy, emailové adresy, telefónne čísla, fotografie a podobne. Zasiahnutých by mohlo byť aj viac ako 350 tisíc ľudí.

Doména webovej stránky kampane Joe Bidena bola znehodnotená útočníkom z Turecka

Útočník z Turecka znehodnotil jednu z domén novo-zvoleného amerického prezidenta Joe Bidena na webovej stránke jeho kampane. Doména vote.joebiden.com bola súčasťou oficiálneho webu kampane. 18. novembra 2020 údajne začala subdoména zobrazovať správu v turečtine. V tejto správe hacker tvrdí, že je „RootAyy1ld1z“, „turecký a moslimský defacer“, ktorý nie je skupinou ani organizáciou, ale „bojuje sám“. Od 23. novembra zostáva doména neprístupná. Za zmienku stojí, že hlavný web kampane nového prezidenta, joebiden.com, nebol ovplyvnený. Aj keď nič nenasvedčuje tomu, ako sa útočník dostal na web, populárne metódy kompromitácie môžu napríklad zahŕňať chyby zabezpečenia v doplnkoch tretích strán.

Bola zverejnená databáza s prihlasovacími údajmi do Spotify. Údaje boli pravdepodobne získané nelegálne.

Výskumný tím vpnMentor objavil otvorenú databázu Elasticsearch obsahujúcu viac ako 380 miliónov záznamov vrátane prihlasovacích údajov a ďalších údajov používateľov, ktoré sú aktívne používané na prihlasovanie do Spotify. Databáza obsahovala viac ako 72GB údajov zahŕňajúc používateľské mená, heslá, emailové adresy a krajiny pobytu. Databáza patrila tretej strane, ktorá ju používala na ukladanie prihlasovacích údajov Spotify, pričom tieto údaje boli pravdepodobne získané nelegálne alebo potenciálne unikli z iných zdrojov.

TLP: White

Unikli údaje z detskej online hry Animal Jam. Zverejnených bolo približne 7 miliónov záznamov.

Spoločnosť WildWorks oznámila, že detská hra Animal Jam utrpela únik údajov. Útočníkom sa podarilo získať prístup k dvom databázam „game_accounts“ a „users“, pričom ukradli približne 46 miliónov záznamov. Dáta obsahovali údaje ako prezývky, šifrované heslá pomocou SHA1, IP adresy z ktorých sa používatelia pripájali a podobne. Spoločnosť zareagovala pohotovo, pričom vytvorila stránku, ktorá podrobne popisuje, čo bolo odcudzené, smeruje používateľov na aktualizáciu hesiel a ponúka pomoc postihnutým osobám. Útočníci zverejnili približne 7 miliónov záznamov.

Na čiernom trhu sa objavila databáza platformy RedDoorz s 5,8 miliónmi záznamov

Po septembrovom útoku na platformu RedDoorz útočník predával databázu obsahujúcu 5,8 miliónov záznamov o používateľoch. Útočník zverejnil vzorku tejto databázy, ktorá obsahovala štruktúru tabuľky a 587 záznamov. Zverejnené dáta obsahovali emailovú adresu používateľa, šifrované heslá pomocou bcrypt, celé meno, pohlavie, odkaz na profilovú fotografiu, telefónne čísla, dátum narodenia a zamestnanie používateľa.

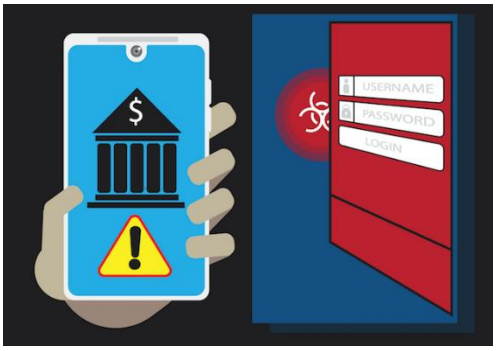
Nesprávna konfigurácia Cloud Hospitality môže ohroziť hostí hotelov po celom svete

CLOUD HOSPITALITY SERVICES

Nesprávna konfigurácia cloudu „Cloud Hospitality“ spoločnosti Prestige Software ohrozila dáta používateľov rezervačných platforiem. Tento cloud využívajú hotely na integráciu svojich rezervačných systémov s webmi ako napríklad Expedia, Booking.com, Hotels.com, Amadeus a podobne. Incident celkovo ohrozil údaje o veľkosti 24,4GB. Platforma používaná na rezerváciu hotelov odhalila 10 miliónov súborov týkajúcich sa hostí rôznych hotelov po celom svete. Záznamy obsahujú citlivé údaje vrátane údajov o kreditnej karte. Dotknutí hoteloví hostia by mohli byť terčom širokej škály útokov, od krádeže identity až po phishing zameraný na krádež dovolenky.

TLP: White

Nový trójsky kôň pre Android s názvom Ghimob je schopný špehovať až 153 aplikácií



Nový bankový trójsky kôň Ghimob sa zameriava na používateľov Androidu. Má schopnosť špehovať 153 mobilných aplikácií od rôznych bánk, kryptomien a búrz. Pomocou tohto trójskeho koňa sú útočníci schopní obísť bezpečnostné opatrenia s cieľom uskutočňovať podvodné transakcie na smartfóne obete. Zatiaľ sú evidované obete v Brazílii, ale predpokladá sa, že sa trójsky kôň rozšíri aj do ďalších krajín. Ghimob má schopnosť nahrávania obrazovky, ktorá mu umožňuje zaznamenávať používateľa pri zadávaní vzoru uzamknutia obrazovky a neskôr ho znova prehrať, aby odomkol zariadenie. Je schopný tiež zabrániť používateľovi odinštalovať ho, reštartovať alebo vypnúť zariadenie.

Útočníci predávali na fórach databázu webovej stránky 123RF. Obsahovala 8,3 miliónov záznamov

Webová stránka 123RF utrpela únik údajov, pričom útočníci predávali na fórach databázu obsahujúcu 8,3 miliónov záznamov o používateľoch. Jedná sa o populárnu webovú stránku, ktorá poskytuje fotografie, obrázky, videá a zvuk na použitie na webových stránkach, pri tlači alebo vo videách. Databáza, ktorá unikla zahŕňa údaje ako celé meno, emailovú adresu, hašované heslá pomocou MD5, názov spoločnosti, telefónne číslo, adresu, PayPal email a IP adresu. V spoločnosti došlo k narušeniu servera umiestneného v jej dátovom centre. Zdá sa, že uniknutá databáza je pravdepodobne zastaraná a nejedná sa o najnovšiu verziu z roku 2020.

Zo služby Pluto TV bolo ukradnutých 3,2 miliónov záznamov o používateľoch

Útočník ukradol 3,2 milióna záznamov o používateľoch Pluto TV. Pluto TV je služba internetovej televízie, ktorá vysiela bezplatné televízne programy s reklamami. Za týmto únikom stojí pravdepodobne útočník alebo

skupina útočníkov s prezývkou „ShinyHunters“, ktorý bol zodpovedný za mnoho únikov dát a za hacknutie súkromného úložiska GitHub spoločnosti Microsoft. Uniknuté údaje zahŕňajú informácie ako meno, emailová adresa, hašované heslo pomocou bcrypt, dátum narodenia, platformu zariadenia a IP adresu. Avšak údaje v tejto zverejnenej databáze sa zdajú byť dva roky staré.

Falošné balíčky modov pre hru Minecraft znemožňujú bežné používanie telefónu. Zasiahnutých je viac ako 1 milión zariadení.

Podvodníci obišli ochranu spoločnosti Google pre oficiálny obchod Play a zverejnili viac ako 20 falošných balíkov modov pre hru Minecraft. Tieto balíčky nedoručujú do smartfónov malvér, avšak po nainštalovaní môžu znemožniť bežné používanie telefónu. Po inštalácii zobrazujú reklamy na celú obrazovku. Mnoho používateľov si neuvedomovalo, že sa jedná o podvod. Medzi podvrhnuté balíčky patria napríklad „Zone Modding Minecraft“, „Textures for Minecraft ACPE“, „Seeded for Minecraft ACPE“, „Mods for Minecraft ACPE“ a „Darcy Minecraft Mod“, pričom sú už odstránené z oficiálneho obchodu Google Play. Zasiahnutých je viac ako 1 milión zariadení so systémom Android.

- **Predajca softvéru pre elektronický obchod X-Cart utrpel koncom októbra útok ransomvérom.**
- **Taiwanská spoločnosť Compal, ktorá vyrába notebooky pre niektoré svetové značky, čelila útoku ransomvérom.**
- **Útok na server Microsoft Exchange v Kuvajte odhalil dve predtým neevidované zadné vrátka Powershellu.**
- **Útočníci využívajú škodlivé falošné reklamy na aktualizáciu Microsoft Teams, aby infikovali systémy zadnými vrátkami kvôli následnému nasadeniu Cobalt Strike.**
- **Kybernetický útok na zdravotnú sieť University of Vermont (UVM) pozastavil vykonávanie rôznych druhov vyšetrení.**
- **Bezpečnostní výskumníci spoločnosti Sonatype objavili npm balík obsahujúci škodlivý kód na odcudzenie citlivých súborov z prehliadačov a aplikácie Discord.**
- **Chyby v doplnku Ultimate Member pre Wordpress môžu viesť k prevzatiu viac ako 100 tisíc stránok.**
- **Viac ako 2800 elektronických obchodov so zastaraným softvérom Magento bolo zasiahnutých útočníkmi.**
- **Na Facebooku sa zjavili reklamy, ktoré hrozili zverejnením ukradnutých dát zo spoločnosti Campari.**
- **Za nedávnymi vlnami ransomvéru na izraelské spoločnosti stoja iránski útočníci.**
- **Útočníci, ktorí stoja za ransomvérom DarkSide tvrdia, že v Iráne vytvárajú distribuovaný úložný systém na ukladanie uniknutých údajov obetí.**
- **Amazon podal žalobu na osobnosti Instagramu a TikTok za údajnú účasť na predaji falošného luxusného tovaru.**
- **Rusky hovoriaci útočníci používajú nový malvér Jupiter na odcudzenie informácií z rôznych softvérov.**
- **Útočník ukradol 2 milióny amerických dolárov z kryptomenovej služby Akropolis.**

- Spoločnosť North Face detegovala útok na svoje webové stránky.
- Schneider Electric varuje pred novým malvérom pre Linux s názvom Drovorub.
- Malvér Lazarus útočí na juhokórejské dodávateľské reťazce.
- Chyba API na zoznamovacej stránke odhalila osobné informácie používateľov.
- Nová čínska APT skupina Funnydream infikovala malvérom viac ako 200 systémov po celej juhovýchodnej Ázii.
- Čínska skupina APT10 využíva zraniteľnosť ZeroLogon proti japonským organizáciám.
- Nový malvér Chaes je zameraný na latinskoamerických používateľov elektronického obchodu.
- Ransomvér REvil zasiahol poskytovateľa hostingu Managed.com.
- Výskumníci z Palo Alto Networks identifikovali viac ako 20 Amazon Web Services API, cez ktoré môžu uniknúť citlivé dáta.
- Ransomvér Egregor po útoku tlačí hodnotu výkupného zo všetkých dostupných tlačiarní, aby si získal pozornosť obete.
- Z aplikácie Pray.com pre veriacich kresťanov unikli súkromné údaje viac ako 10 miliónov ľudí.
- FBI varuje pred zvýšenou aktivitou ransomvéru Ragnar Locker.
- Nový útok s názvom LidarPhone používa na odpočúvanie robotické vysávače.
- Únik údajov spoločnosti Luxottica zasiahol 820 tisíc pacientov EyeMed a LensCrafters.
- Malvér Gootkit sa vracia k životu spolu s ransomvérom REvil.
- Útočníci zverejnili viac ako 4,2 milióna používateľských účtov aplikácie Peatix.
- Nový malware WAPDropper zneužíva zariadenia Android na podvody s WAP.

- **TrickBot sa aktualizuje, aby prežil pokusy o zastavenie jeho šírenia.**
- **Linuxový malvér skupiny Stantinko sa vydáva za webový server Apache.**
- **Aplikácie Baidu v službe Google Play utrpeli únik citlivých údajov.**
- **Útočníci oklamali zamestnancov GoDaddy v operácii zameranej na kompromitáciu kryptomenových služieb NiceHash a Liquid.**
- **Canon verejne potvrdil augustový útok ransomvérom.**

Závažné zraniteľnosti bežných softvérových produktov

Spoločnosť Oracle dodatočne po vydaní plánovanej štvrťročnej aktualizácie opravila kritickú zraniteľnosť

Spoločnosť Oracle vydala záplatu na kritickú zraniteľnosť, ktorá umožňuje vzdialené vykonávanie kódu. Ovplyvňuje niekoľko verzií servera Oracle WebLogic. Môže byť zneužitá prostredníctvom protokolu HTTP bez autentifikácie.

Spoločnosť Google opravila niekoľko zraniteľností v prehliadači Chrome, pričom dve z nich sú typu zero-day

Spoločnosť Google vydala záplatu pre niekoľko chýb zabezpečenia. Dve z nich sú typu zero-day, pričom zneužitie prvej môže viesť ku vzdialenému vykonávaniu kódu. Táto zraniteľnosť sa nachádza v komponente V8 pre prehliadač Chrome, pričom súvisí s jeho nesprávnou implementáciou. Ďalšia zero-day zraniteľnosť sa nachádza v prehliadači Chrome pre systém Android. Môže spôsobiť pretečenie medzipamäte haldy.

Spoločnosť Apple vydala záplatu pre tri zero-day zraniteľnosti ovplyvňujúce rôzne druhy zariadení

Bezpečnostný tím spoločnosti Google odhalil tri zero-day zraniteľnosti v zariadeniach od spoločnosti Apple. Prvá zraniteľnosť sa týka knižnice FontParser, pričom môže viesť k poškodeniu pamäte, ďalšia súvisí s eskaláciou privilégií v jadre iOS, čo umožňuje vykonávanie ľubovoľného kódu a posledná môže viesť k úniku pamäte.

Spoločnosť Oracle opravila 402 zraniteľností v októbrových aktualizáciách

Softvérová spoločnosť Oracle vydala v októbri množstvo aktualizácií, ktoré opravujú až 402 chýb v jej produktoch. Dvojica chýb (CVE-2020-1953 a CVE-2020-14871) dosiahla skóre CVSS 10, kritických je aj mnoho ďalších chýb. Ako uvádza portál

Threatpost.com, viac ako polovicu zraniteľností je možné zneužiť na diaľku bez autentifikácie.

Za posledné tri týždne spoločnosť Google opravila už štvrtú a piatu zero-day zraniteľnosť v prehliadači Chrome

Google Chrome

Závažné zraniteľnosti sa nachádzajú v prehliadači Chrome. CVE-2020-16013 súvisí s nesprávnou implementáciou komponentu V8, pričom môže viesť k vzdialenému vykonávaniu kódu. CVE-2020-16017 sa týka komponentu, ktorý slúži na izoláciu údajov rôznych webových stránok a jej zneužitie môže spôsobiť poškodenie pamäte a umožniť vykonávanie ľubovoľného kódu.

V IOS XR od spoločnosti Cisco sa nachádza zraniteľnosť, ktorej zneužitie môže viesť k nefunkčnosti smerovačov Cisco ASR série 9000

Zraniteľnosť nachádzajúca sa v IOS XR verzie nižšej ako 6.7.2 alebo 7.1.2 umožňuje vzdialeným útočníkom znefunkčniť smerovače Cisco ASR série 9000. Chyba vzniká nesprávnym pridelením prostriedkov pri spracovávaní sieťového prenosu a vo všeobecnosti môže viesť k narušeniu dostupnosti služby.

V aplikácii Cisco Security Manager sa vyskytujú tri zraniteľnosti. Na dve z nich vydala spoločnosť záplatu.

Spoločnosť Cisco vydala záplatu na dve z troch objavených zraniteľností v aplikácii Cisco Security Manager. Obe opravené zraniteľnosti môžu útočníkovi umožniť neoprávnený prístup k citlivým údajom. Posledná neopravená zraniteľnosť sa týka Java funkcie, ktorá slúži na deserializáciu obsahu dodávaného používateľom. V prípade zneužitia je útočník schopný vzdialene vykonávať kód.

V produktoch spoločnosti VMware bola odhalená kritická a závažná zraniteľnosť

V produktoch ESXi, Fusion, Workstation a VMware Cloud Foundation sa vyskytuje zraniteľnosť, ktorá sa týka použitia odalokovaného miesta v pamäti. Ovplyvňuje XHCI USB kontrolér, pričom jej zneužitie môže viesť k vykonávaniu ľubovoľného kódu

na cieľovom systéme. Ďalšia chyba v produktoch spoločnosti VMware sa týka spôsobu správy systémových volaní a jej zneužitie môže viesť k zmene oprávnení v systéme.

Kritické zraniteľnosti Cisco

V produktoch Cisco bolo opravených viacero závažných zraniteľností a 4 kritické:
CVE-2020-27130: Jedná sa o zraniteľnosť v softvéri Cisco Security Manager a umožňuje neautentizovanému vzdialenému útočníkovi získať prístup a upraviť citlivé informácie. Je spôsobená nesprávnym overením postupnosti znakov v požiadavkách na príslušné zariadenie.
CVE-2020-3470: Viaceré chyby v podsystéme API ovládača Cisco Integrated Management Controller (IMC) môžu umožniť neautentizovanému útočníkovi vzdialene vykonávať kód s administrátorskými oprávneniami. Sú spôsobené nesprávnou hraničnou kontrolou určitého vstupu dodaného používateľom.
CVE-2020-3586: Zraniteľnosť webového rozhrania na správu aplikácie Cisco DNA Spaces Connector môže útočníkovi umožniť vzdialene vykonávať kód bez akejkoľvek autentizácie. Je spôsobená nedostatočným overovaním vstupu zadaného používateľom v tomto webovom rozhraní.
CVE-2020-3531: Zraniteľnosť v REST API aplikácie Cisco IoT Field Network Director (FND) môže umožniť vzdialenému útočníkovi prístup k back-end databáze zraniteľného systému. Je spôsobená tým, že ovplyvnený softvér nesprávne overuje volania REST API.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero rôznych kritických a závažných zraniteľností, z toho kritické boli nasledujúce 2:
CVE-2020-12321: Nesprávne obmedzenie vyrovnávacej pamäte v niektorých produktoch Intel® Wireless Bluetooth® pred verziou 21.110 môže umožniť neautentizovanému používateľovi povoliť eskaláciu privilégií.
CVE-2020-8752: Zápis mimo povolených hodnôt v podsystéme IPv6 pre Intel® AMT, Intel® ISM verzie pred 11.8.80, 11.12.80, 11.22.80, 12.0.70 a 14.0.45 môže umožniť neoprávnenému používateľovi povoliť eskaláciu privilégií prostredníctvom prístupu do siete.

Mesačník zraniteľností November 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
    - Spoločnosť Oracle dodatočne po vydaní plánovanej štvrťročnej aktualizácie opravila kritickú
      zraniteľnosť
    - Spoločnosť Google opravila niekoľko zraniteľností v prehliadači Chrome, pričom dve z nich sú
      typu zero-day
    - Spoločnosť Apple vydala záplatu pre tri zero-day zraniteľnosti ovplyvňujúce rôzne druhy zariadení
    - Spoločnosť Oracle opravila 402 zraniteľností v októbrových aktualizáciách
    - Za posledné tri týždne spoločnosť Google opravila už štvrtú a piatu zero-day zraniteľnosť v prehliadači Chrome
    - V IOS XR od spoločnosti Cisco sa nachádza zraniteľnosť, ktorej zneužitie môže viesť k nefunkčnosti smerovačov Cisco ASR série 9000
    - V aplikácii Cisco Security Manager sa vyskytujú tri zraniteľnosti. Na dve z nich vydala spoločnosť záplatu.
    - V produktoch spoločnosti VMware bola odhalená kritická a závažná zraniteľnosť

https://www.csirt.gov.sk/aktualne-7d7.html?id=231