MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

Október 2020

Vypracoval: CSIRT.SK

TLP: White

Počas mesiaca október bolo odhalených mnoho útokov pomocou ransomvéru Ryuk. Tento ransomvér používajú útočníci na získanie a následné šifrovanie rôznych dát v rôznych odvetviach. V tomto mesiaci sme mohli vo svete zaregistrovať útoky využívajúce Ryuk na niekoľko spoločností a tiež na nemocnice. Podľa zverejnených údajov od spoločností Check Point a IBM Security X-Force Incident Response sú na čele zoznamu najpoužívanejších za tretí kvartál 2020 práve ransomvéry Ryuk, Maze a REvil.

Ransomvér Ryuk bol prvýkrát objavený v roku 2018, pričom od júla 2020 jeho aktivita len stúpa. V dnešnej dobe útočí na približne 20 organizácií za týždeň. Vzhľadom k tomu, že zdravotníctvo dnes významne získava na dôležitosti, skupiny využívajúce Ryuk sa vo väčšine svojich útokov zamerali práve na zdravotnícke organizácie za účelom zisku financií.

Zdravotnícke stredisko Sky Lakes v Oregone a St. Lawrence v New Yorku boli zasiahnuté útokmi týmto ransomvérom, čo dokonca ovplyvnilo liečbu pacientov. Minulý mesiac bol zasiahnutý Ryukom reťazec Universal Health Services, čo ovplyvnilo cez 200 zdravotníckych zariadení po celej Amerike. Za týmito útokmi stojí skupina s názvom UNC1878. Práve kvôli týmto útokom mohli pacienti zaznamenať predĺžený čas čakania na poskytnutie starostlivosti.

Universal Health Services (UHS) tvrdí, že sa im podarilo obnoviť systémy po septembrovom útoku ransomvérom Ryuk. Od samotného útoku boli spojazdnené najviac postihnuté výpočtové systémy v nemocniciach s behaviorálnou a akútnou starostlivosťou a tiež systémy potrebné pre operácie, laboratórium a správu záznamov pacientov.

Ďalšími zdravotníckymi strediskami, ktoré utrpeli útok ransomvérom Ryuk sú Wyckoff Heights Medical Center v Brooklyne a University of Vermont Health Network. Wyckoffova nemocnica sa rozhodla vypnúť časť svojej siete, avšak ransomvér stihol zašifrovať súbory na mnohých zariadeniach. Nie je však známe, aký dopad tento útok mal na liečbu pacientov. Čo sa týka University of Vermont Health Network, ransomvér zasiahol v rôznej miere všetky nemocnice v tejto sieti. Medzi postihnuté nemocnice patria napríklad Alice Hyde Medical Center v Malone v New Yorku, Central Vermont Medical Center v Berlíne alebo Porter Medical Center v Middlebury.

Ukázalo sa, že posledný októbrový týždeň bol pre americké zdravotníctvo naozaj veľmi nepríjemným. Dokopy bolo okrem niekoľkých útokov na rôzne spoločnosti zaznamenaných šesť útokov na nemocnice v USA.

Jednou zo zasiahnutých spoločností ransomvérom Ryuk mimo zdravotníctva je Steelcase, ktorá sprostredkúva kancelársky nábytok. Spoločnosť pohotovo zareagovala, pričom dočasne odstavila dotknuté systémy a súvisiace operácie. Spoločnosť Steelcase neevidovala žiadnu stratu údajov, a teda sa predpokladá, že útok mal nízky dopad.

Európska spoločnosť pôsobiaca v oblasti informačných technológií Sopra Steria tiež potvrdila, že sa stala obeťou útoku ransomvérom Ryuk. Sopra Steria zamestnáva viac ako 46 tisíc zamestnancov vo viac ako 25 krajinách. Spoločnosť uviedla, že ich vyšetrovanie nenaznačuje, že by v súčasnosti došlo k

úniku akýchkoľvek údajov o zákazníkoch. Útočníci najprv kompromitovali sieť a následne nasadili ransomvér do jej systémov.

Priemerná suma, ktorú skupina stojaca za ransomvérom Ryuk od svojich obetí dostala, je 48 bitcoinov (cca 750 tisíc amerických dolárov). Od roku 2018 zarobili najmenej 150 miliónov dolárov. Najväčšia potvrdená suma, ktorú im obete zaplatili, bolo 2 200 bitcoinov, čo v súčasnosti prestavuje takmer 34 miliónov amerických dolárov.

Celý útok ransomvérom Ryuk začína prvotným zaslaním phishingového emailu obeti, pričom sa do zariadenia stiahne BazarLoader. Ten vykonáva prieskum na infikovanom zariadení pomocou rôznych nástrojov. Ďalším z hlavných bodov je použitie nástroja Cobalt Strike. Následne sa deaktivuje Windows Defender cez Powershell a Ryuk je spustený minútu po prenesení cez Server Message Block (SMB). Po spustení šifrovania sú najskôr zasiahnuté servery určené na ukladanie záloh. Následne je cez port SMB Ryuk prenesený na zvyšné servery a na spustenie je použité RDP pripojenie.

Spoločnosť Microsoft sa pokúšala narušiť botnet TrickBot, ktorý spočiatku slúžil na distribúciu tohto ransomvéru. Na niektoré infikované zariadenia doručili neštandardný konfiguračný súbor, ktorý im dal pokyn, aby sa pripojili na C&C server s IP adresou 0.0.0.1 na TCP porte 1. Neznámy počet botov tak ostal izolovaný od siete a stali sa tak nedostupnými z pôvodného C&C servera. Cieľom tohto kroku bolo zničiť botnet TrickBot a ochrániť tak nadchádzajúce voľby v USA. V nadväznosti na to útočníci začali na distribúciu svojho ransomvéru používať nového trójskeho koňa nazývaného BazarLoader alebo BazarBackdoor.

Riešené incidenty na Slovensku a z našej činnosti

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

Okrem toho riešila vládna jednotka prípady zraniteľností objavených na niekoľkých webových stránkach štátnej správy. Zraniteľnosti boli po upozornení v krátkom čase odstránené. Uprostred mesiaca sa v štátnej správe začali šíriť podozrivé emaily s legitímnou historickou komunikáciou a podpisom dvoch obcí. CSIRT.SK tento incident riešil aj v širšej miere na úrovni kraja, do ktorej prerástol po získaní hlbšieho vhľadu do situácie. Pritom poskytol súčinnosť orgánom činným v trestnom konaní. Svojej konštituencii rozposlal upozornenie a odporučil zvýšenú obozretnosť pri manipulácii s predmetnou emailovou komunikáciou.

Jednotka CSIRT.SK v tomto mesiaci zaznamenala masívnu phishingovú kampaň šíriacu ransomvér Emotet. V rámci svojej proaktívnej činnosti kontaktovala organizácie vo svojej konštituencii. Jednotka analyzovala niekoľko vzoriek malvéru z kampane a svojej konštituencii rozposlala získané indikátory kompromitácie, vrátane hašov a názvov škodlivých súborov, IP adries a domén odkiaľ bol malvér distribuovaný a adries C&C serverov. CSIRT.SK sa ďalej zameral na bezpečnosť v zdravotníckom sektore. Vzhľadom na súčasnú epidemiologickú situáciu je zachovanie jeho plnej funkčnosti zásadné.

Významné útoky vo svete

IPStorm infikoval dokopy viac ako 13 500 zariadení vo viac ako 84 krajinách

IPStorm je botnet s malvérom, ktorý bol prvýkrát zaznamenaný minulý rok v zameraní na operačné systémy Windows. Vyvinul sa natoľko, že je schopný infikovať aj ďalšie typy platforiem vrátane Android, Linux a Mac. Podarilo sa mu infikovať viac ako 13500 zariadení vo viac ako 84 krajinách. Malvér bol napísaný v jazyku Go, a teda je jedným z mála kmeňov malvérov tohto druhu. IPStorm sa zameriava momentálne na platformu Android, pričom skenuje internet na zariadenia, ktoré majú otvorený port ADB (Android Debug Bridge). Platformy Linux a Mac zariadení sú infikované po tom, čo IPStorm vykoná slovníkové útoky na SSH. Malvér následne zvyčajne skontroluje, či je prítomný honeypot, získa perzistenciu pri zavádzaní operačného systému, a potom zabije procesy, ktoré by mohli narušiť jeho činnosť. Nie je však celkom známe, aký je konečný cieľ tohto botnetu, pretože nebola identifikovaná ďalšia škodlivá činnosť aj napriek tomu, že si necháva zadné vrátka do infikovaných zariadení.

Bola objavená nová APT skupina s názvom XDSpy, ktorá zostala neodhalená 9 rokov

Spoločnosť ESET objavila novú APT skupinu s názvom XDSpy, ktorá zostala neodhalená 9 rokov. Primárnym cieľom tejto skupiny je prieskum a následná krádež dokumentov. XDSpy sa zamerala na vládne agentúry a súkromné spoločnosti vo východnej Európe a na Balkáne. Hlavným používaným nástrojom skupiny je súbor malvérových nástrojov, ktorý pomenovali XDDown. Balík XDDown slúžil ako nástroj na sťahovanie škodlivého kódu na infikovanie obete a na následné sťahovanie sekundárnych modulov. Medzi tieto moduly patria XDREcon, XDList, XDMonitor, XDLoc, XDPass, ktoré slúžia na extrakciu a zhromažďovanie rôznych informácií o počítači. Na infikovanie používali spearphishingové emailové kampane, pričom emaily obsahovali škodlivé súbory typu Powerpoint, JavaScript, zip alebo lnk.

Facebook odhalil niekoľko tajomstiev malvéru SilentFade

Malvér SilentFade bol identifikovaný koncom roka 2018, pričom spoločnosť Facebook podnikla v decembri 2019 právne kroky proti útočníkom. Malvér využíval chybu na strane servera, aby trvale potlačil upozornenia a zaistil, aby infikovaní používatelia neboli informovaní o podozrivej aktivite súvisiacej s ich účtami. To umožnilo SilentFade zneužiť napadnuté účty a spustiť škodlivé reklamy bez toho, aby si obete niečo všimli. Aj keď bol malvér prvýkrát odhalený v poslednom týždni roku 2018, predpokladá sa, že skupina útočníkov, ktorá za ním stojí, funguje od roku 2016. Neustále sa prispôsobuje novým funkciám Facebooku a pravdepodobne sa rozšíri aj na ďalšie sociálne platformy a webové služby.

Niektoré webové stránky v rebríčku Alexa TOP 10000 boli infikované

Vyšetrovanie v rebríčku Alexa Top 10000 odhalilo, že veľa z populárnych webov bolo infikovaných malvérom, ktorý ťaží kryptomeny a skriptmi na skimming kreditných kariet. Medzi poškodené stránky patria napríklad libero[.]it, pojoksatu[.]id a www[.]heureka[.]cz. Návšteva infikovanej stránky s takýmto skriptom môže okamžite zvýšiť využitie procesora. V spoločnosti Palo Alto Networks spozorovali prípady niekoľkých reklám na legitímnom webe ojazdených vozidiel libero[.]it, ktoré boli upravené tak, aby obsahovali odkazy, ktoré používateľov presmerovali na škodlivú stránku obsahujúcu skript na ťažbu mincí JSEcoin. Avšak prevádzka JSEcoin bola ukončená v apríli 2020, a teda útočníci už nie sú schopní prijímať vyťažené mince.

Štyri balíčky npm v JavaScripte obsahovali škodlivý kód

Boli odhalené štyri balíčky npm v JavaScripte obsahujúce škodlivý kód, ktorý zhromažďoval podrobnosti o používateľoch a nahrával informácie na GitHub. Medzi štyri balíčky patria „electorn“, „lodashs“, „loadyaml“ a „loadyml“. Všetky balíčky boli vyvinuté

používateľom „simplelive12“, pričom dva z nich boli odstránené krátko po zverejnení. Zvyšné dva boli odstránené neskôr bezpečnostným tímom npm. Tieto škodlivé balíky zhromažďujú údaje ako IP adresa, krajina, mesto, používateľské meno počítača, cestu k domovskému adresáru a informácie o modeli procesora. Následne ich zverejnia ako nový komentár v časti „Problémy“ na úložisku. Je vysoko odporúčané skontrolovať závislosti projektov či náhodou neobsahujú jeden z týchto štyroch balíčkov.

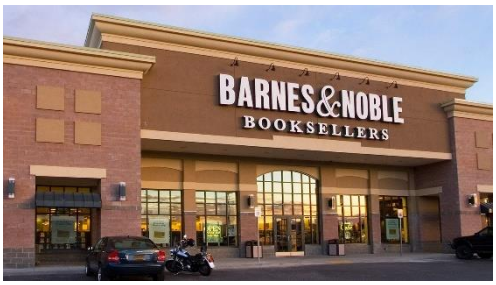
Kvôli útoku ransomvérom na spoločnosť eResearchTechnology bol spomalený výskum ohľadom COVID-19

Útok ransomvérom na spoločnosť eResearchTechnology potenciálne spomalil výskum ohľadom koronavírusu na celom svete. Táto spoločnosť dodáva farmaceutickým spoločnostiam nástroje na vykonávanie klinických testov vrátane testov na vakcíny proti COVID-19. Zasiahnuté boli spoločnosti IQVIA a Bristol Myers Squibb, avšak vďaka zálohovaniu dát bol dopad útoku obmedzený. Našli sa však aj spoločnosti, ktoré týmto útokom ostali postihnuté. Nie je celkom jasné, aká bola motivácia útoku. Útoky na zdravotnícke organizácie stále pokračujú.

Spoločnosť Software AG utrpela únik dát o veľkosti cca 1TB

Ransomvér Clop zasiahol sieť nemeckého gigantu Software AG. Spoločnosť tvrdí, že zasiahnutá bola len vnútorná sieť, a teda cloudové služby zostali nedotknuté. Rôzne údaje boli stiahnuté zo serverov a notebookov zamestnancov spoločnosti. Chat na platobnej stránke spoločnosti ukazuje, že útočníci sa vyhrážajú zverejnením 1TB dát, ktoré údajne ukradli zo zariadení. Dáta zahŕňajú rôzne dokumenty, zmluvy, správy, korešpondenciu a ďalšie citlivé údaje. Útočníci žiadajú výkupné v hodnote približne 23 miliónov dolárov.

Kníhkupectvo Barnes & Nobles utrpelo kybernetický útok. Útočníci získali neoprávnený prístup do systému.



Americké kníhkupectvo Barnes & Noble sa stalo obeťou kybernetického útoku. Zákazníci mali obmedzený prístup do svojej knižnice, kde nevedeli pristúpiť k už zakúpeným elektronickým knihám alebo časopisom. Spoločnosť uviedla, že utrpela zlyhanie systému a usiluje sa o návrat do plnej prevádzky. V rámci útoku získali útočníci neoprávnený prístup k podnikovým systémom. Ukradnuté boli emailové adresy, fakturačné adresy, dodacie adresy a história nákupov. Nebolo potvrdené, že sa jednalo o útok ransomvérom, avšak spoločnosť prevádzkovala Pulse VPN, ktorá bola zraniteľná voči chybe CVE-2019-11510. Tá je častokrát zneužívaná práve v útokoch ransomvérom.

V spoločnosti Dickey's Barbecue Pit došlo k úniku údajov o platobných kartách viac ako 3 miliónov zákazníkov

Podrobnosti o kartách viac ako 3 miliónov zákazníkov spoločnosti Dickey's Barbecue Pit boli zverejnené na trhu s kartami a podvodmi Joker's Stash. Tento únik odhalila spoločnosť Gemini Advisory, ktorá sleduje finančné podvody. Útočníci narušili systém POS (Point-of-Sale) používaný v reštauráciách Dickey. Záznamy o platobných kartách sa väčšinou týkajú kariet využívajúcich technológiu magstripe, pričom karty sa predávajú približne za 17 dolárov za kus.

V právnickej firme Fragomen došlo k úniku údajov o súčasných aj bývalých zamestnancoch spoločnosti Google

Imigračná právnická firma Fragomen, Del Rey, Bernsen & Loewy, LLP zverejnila informácie o útoku, ktorý odhalil osobné údaje súčasných a bývalých zamestnancov spoločnosti Google. Fragomen je jednou z najväčších amerických právnických firiem zaoberajúcich sa imigračným právom. Má viac ako 582 advokátov na 47 miestach po celom svete. Sieť tejto právnickej firmy bola napadnutá, pričom útočník sa dostal k súboru, ktorý obsahoval osobné údaje bývalých

a aktuálnych zamestnancov spoločnosti Google. Všetci zamestnanci v USA musia vyplniť formulár I-9 na vyhlásenie občianstva a spôsobilosti pracovať v tejto krajine. Tento formulár obsahuje informácie ako celé meno zamestnanca, poštovú adresu, dátum narodenia, e-mailovú adresu, telefónne číslo, číslo sociálneho poistenia, čísla pasov a ďalšie identifikačné údaje.

Spoločnosti Ubisoft a Crytek utrpeli útoky, pričom došlo k úniku dát

Údaje získané ransomvérom Egregor zo spoločností Ubisoft a Crytek boli zverejnené na internete. V prípade úniku spoločnosti Ubisoft útočníci zdieľali súbory, aby naznačili, že vlastnia zdrojový kód jednej z hier série Watch Dogs s názvom Legion. Bolo však nemožné overiť, či kód bol skutočne ukradnutý, alebo získaný inou cestou. Zatiaľ čo z Ubisoftu uniklo len 20MB dát, z Cryteku uniklo 300MB dát, pričom tieto údaje obsahovali omnoho viac informácií. Súbory zo spoločnosti Crytek obsahovali dokumenty, ktoré sa zdali byť ukradnuté z divízie vývoja hier ako sú Arena of Fate, Warface a Gface. Útočníci uviedli, že z Ubisoftu boli odcudzené dáta, zatiaľ čo v spoločnosti Crytek boli okrem krádeže aj zašifrované rôzne súbory. Aktuálne sa vyhrážajú, že v prípade, že ich Ubisoft nebude kontaktovať, zverejnia zdrojový kód pripravovaných hier.

V rámci služby Docsketch došlo k neoprávnenému prístupu k databáze

Služba elektronického podpisovania dokumentov Docsketch upozorňuje zákazníkov ohľadom narušenia bezpečnosti, ku ktorému došlo v priebehu leta. Spoločnosť uvádza, že útočníci získali prístup ku kópii databázy, ktorá obsahovala snímku služby Docsketch z 9. júla 2020. Útočník mohol pristúpiť k menám, podpisom, osobným údajom a dokonca aj podrobnostiam o platobných kartách. Databáza navyše obsahovala prihlasovacie údaje a kontakty na používateľov. Spoločnosť uvádza, že už po augustovom prieniku zabezpečila svoj systém.

TLP: White

- Útočník z Ruska, ktorý napadol LinkedIn a Dropbox bol odsúdený na sedem rokov väzenia
- Twitter zaznamenal niekoľko výpadkov, pričom používatelia videli hlášku „Something went wrong“
- Po útoku ransomvérom v Pakistane útočníci zverejnili súbory ukradnuté spoločnosti K-Eletric
- Stovky amerických organizácií obdržalo phishingové emailové správy, za ktorými stojí Emotet
- Spoločnosť H&M dostala pokutu 41 miliónov amerických dolárov za špehovanie pracovníkov
- Útočníci využívajú voľby v USA vo svoj prospech tým, že rozposielajú phishingové emaily s cieľom získať od voličov osobné údaje
- Nemocnica v New Jersey zaplatila útočníkom výkupné v hodnote 670 tisíc, aby zabránila úniku informácií
- Variant botnetu Mirai s názvom Ttint rozšíril svoje schopnosti špionáže, aby doplnil svoje funkcie pre narušenie dostupnosti služby
- Útočníkom sa podarilo ukradnúť výplaty zamestnancov na niekoľkých švajčiarskych univerzitách
- Malvér na ťažbu kryptomien pridáva možnosti krádeže hesiel v operačnom systéme Linux
- Skupiny AgentTesla, LimeRAT, W3Cryptolocker a Redline Stealer používajú Paste.nrecom pri phishingových útokoch
- Spoločnosť Microsoft uviedla, že iránski útočníci zneužívajú zraniteľnosť Zerologon vo svojich kampaniach
- Skupina útočníkov Fullz House napadla webovú stránku Boom!
- Útočníci sa zameriavajú na zariadenia IoT pomocou nového P2P botnetu
- Útočníci kompromitovali ázijskú službu slúžiacu na donášku potravín

- Malvér Waterbear bol používaný pri útokoch na vládne organizácie
- Rusky hovoriaca skupina podniká útoky voči ruským priemyselným organizáciám
- Ransomvér v rámci Androidu zneužíva notifikačné služby na zobrazovanie výkupného
- Školský obvod v americkom štáte Massachusetts sa stal obeťou útoku ransomvérom
- Spoločnosť Sam's Club pravdepodobne utrpela únik údajov
- Ransomvér AndroidOS/MalLocker.B sa na infikovanom zariadení aktivuje po stlačení tlačidla „Home"
- Škodlivé aplikácie pre zariadenia Fitbit môžu byť nahraté na legitímnu Fitbit doménu
- Skupina FIN11 používa nové techniky pri útokoch ransomvérom
- USA obvinilo 14 členov medzinárodnej skupiny QQAAZZ pre pranie špinavých peňazí
- Portorické hasičské oddelenie utrpelo útok na databázu, pričom útočníci požadovali 600 tisíc amerických dolárov ako výkupné
- Boli identifikované nové verzie GravityRAT, ktoré sa zameriavajú na zariadenia s operačným systémom Android a macOS
- Útočníci sa zameriavajú na používateľov služby Office365 s cieľom získať kontrolu nad ich schránkami pomocou protokolu OAuth
- Čínski útočníci sa zameriavajú na zraniteľnosť protokolu Cisco Discovery Protocol
- Ransomvéru LockBit trvá len päť minút spustiť šifrovanie na napadnutých systémoch
- Nórska ministerka zahraničných vecí uviedla, že Rusko stojí za kybernetickým útokom na nórsky parlament (Stortinget)
- Útočníci použili chyby VPN na prístup k podporným systémom volieb v USA

- **Botnet Qbot používa na distribúciu svojho škodlivého softvéru novú šablónu**
- **Spoločnosť Tyler Technologies zaplatila výkupné za dešifrovací kľúč na obnovu súborov**
- **Útočníci ukradli viac ako 22 miliónov amerických dolárov od používateľov peňaženky Electrum**
- **Bývalý americký informátor Edward Snowden získal trvalý pobyt v Rusku**
- **Phishingová kampaň je zameraná na viac ako 50 tisíc používateľov služieb Office365, ktorá ich má informovať o „zmeškanom rozhovore“ od spoločnosti Microsoft Teams**
- **Donaldovi Trumpovi útočník prelomil heslo na Twitteri**
- **Služba Nitro PDF utrpela útok, ktorý ovplyvňuje organizácie ako Google, Apple, Microsoft, Chase a Citibank**
- **Mobilná hra „Among Us“ je pod paľbou rôznych útokov**
- **Aplikácie určené na chat, napríklad LINE, Slack a Twitter DM, môžu zdieľať údaje o polohe a súkromné informácie so servermi tretích strán**
- **Medzinárodnú spoločnosť Enel Group opäť zasiahol útok ransomvérom**
- **Len týždeň pred voľbami v USA útočníci prenikli na webovú stránku s kampaňou Donalda Trumpa**
- **Rusky hovoriaca skupina Turla sa nabúrala do systémov nemenovanej európskej vládnej organizácie**

Závažné zraniteľnosti bežných softvérových produktov

Cisco vydalo záplaty pre aktívne zneužívané DoS zraniteľnosti v IOS XR

Zraniteľnosti triedy DoS môže zneužiť neautentifikovaný útočník a vedú ku zlyhaniu IGMP procesu alebo vyčerpaniu operačnej pamäte. Zneužitie zraniteľností je možné, len ak sa používa multicast routing a zariadenie môže prijímať DVMPR prevádzku.

Kritickú zraniteľnosť v Adobe Flash Player je možné využiť na vzdialené vykonávanie kódu

Zraniteľnosť je spôsobená dereferenciou nulového ukazovateľa a spôsobuje zlyhanie programu Adobe Flash Player. Je možné zneužiť ju aj na vykonanie kódu, ktorý je možné poslať aj vzdialene v HTTP odpovedi, ktorú Flash Player spracuje.

VMware - kritické zraniteľnosti v ESXi, Workstation, Fusion a NSX-T

Spoločnosť VMware odstránila zraniteľnosti vyskytujúce sa v ESXi, Workstation, Fusion a NSX-T. Tieto chyby vo všeobecnosti môžu viesť k vzdialenému vykonávaniu kódu na zraniteľných zariadeniach. Útočníci tiež môžu získavať rôzne informácie, eskalovať oprávnenia, prípadne môže dôjsť k narušeniu dostupnosti služby. Na serveri vCenter dochádza k chybe funkcie zabezpečenia pri aktualizácii. Útočník je teda schopný prevziať kontrolu nad spojením.

Spoločnosť Google vydala záplatu na zero-day zraniteľnosť v prehliadači Chrome. Môže spôsobiť poškodenie pamäte.

Kvôli kritickej zero-day zraniteľnosti v prehliadači Chrome, konkrétne v knižnici FreeType, môže dôjsť k pretečeniu medzipamäte haldy, čo spôsobuje poškodenie pamäte zariadenia. Útočníci môžu chybu zneužiť na vykonávanie ľubovoľného kódu.

NAS zariadenia od spoločnosti QNAP obsahujú 2 kritické zraniteľnosti

Obe kritické zraniteľnosti sa nachádzajú v aplikácii Helpdesk a sú spôsobené nesprávnou kontrolou prístupu. Vzdialený útočník môže zraniteľnosti zneužiť na získanie kontroly nad sieťovými úložnými zariadeniami (NAS).

Zraniteľnosti Intel

V produktoch Intel bola opravená jedna kritická a jedna závažná zraniteľnosť. Kritická má CVSS skóre 9.8:
CVE-2020-8758: Táto zraniteľnosť môže neoprávnenej osobe umožniť eskaláciu privilégií prostredníctvom prístupu do siete. Chyba sa vyskytuje v Intel(R) AMT a Intel(R) ISM vo verziách pred 11.8.79, 11.12.79, 11.22.79, 12.0.68 a 14.0.39.

Mesačník zraniteľností Október 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
    - Cisco vydalo záplaty pre aktívne zneužívané DoS zraniteľnosti v IOS XR
    - Kritickú zraniteľnosť v Adobe Flash Player je možné využiť na vzdialené vykonávanie kódu
    - VMware - kritické zraniteľnosti v ESXi, Workstation, Fusion a NSX-T
    - Spoločnosť Google vydala záplatu na zero-day zraniteľnosť v prehliadači Chrome. Môže spôsobiť poškodenie pamäte.
    - NAS zariadenia od spoločnosti QNAP obsahujú 2 kritické zraniteľnosti

https://www.csirt.gov.sk/aktualne-7d7.html?id=229