ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Marec 2019

Vypracoval: CSIRT.SK

TLP: White

V prvom štvrťroku 2019 sa vyrojilo mnoho výročných správ a štatistík od rôznych bezpečnostných spoločností, hodnotiacich stav kybernetickej bezpečnosti v roku 2018. Mimo to sa objavilo niekoľko zaujímavých tohtoročných prípadov. Pozrime sa teda na dianie v oblasti bezpečnosti osobných a prihlasovacích údajov a prienikov do osobných účtov na webstránkach.

Niekoľko zaujímavých informácií priniesol článok portálu Darkreading.com. Hneď začiatkom roku zverejnil istý útočník na darkwebovom obchode obrovskú zbierku prihlasovacích údajov, párov e-mail – heslo, ktoré boli zozbierané z predchádzajúcich prienikov do databáz používateľov mnohých webstránok. Zbierka obsahovala 87 GB dát a dostala názov Collection #1. Krátko na to nasledovali ďalšie dve kolekcie s oveľa väčším rozsahom. Tento mesiac sa pridala Collection #4 (viď správu v časti Významné útoky vo svete). Správa spoločnosti Proofpoint ukazuje, že prienik do účtov s využitím phishingu vzrástol v roku 2018 na dvojnásobok oproti predchádzajúcemu roku a na trojnásobok oproti roku 2016. Začiatkom roka 2019 tvorili prihlasovacie údaje až pätinu celkovo odcudzených údajov a malvér zameraný na ich krádež tvoril takmer polovicu škodlivého kódu šíriaceho sa online.

Odcudzené údaje potom útočníci využijú na tzv. „credential stuffing“ útok, pri ktorom sa pokúšajú s týmito údajmi prihlásiť do rôznych online služieb. Tieto útoky sú efektívnejšie, ako útoky hrubou silou, pretože používatelia veľmi často zvyknú „recyklovať“ svoje heslá a používať rovnaké heslá pre mnohé služby. Pretože vytváranie a pamätanie si desiatok rôznych hesiel môže byť komplikovaná záležitosť, je táto chyba pochopiteľná. Dá sa jej však jednoducho vyhnúť používaním manažérov hesiel, akým je napríklad KeePass. Spoločnosť Akamai zaznamenala minulý rok za obdobie dva mesiace vyše 8 miliárd škodlivých pokusov o prihlásenie do kont svojich klientov. Zväčša sa jednalo o pomerne malé množstvo požiadaviek, aby sa útočníci vyhli detekcii, no zaznamenali tiež píky od botnetu s 300 000 požiadavkami za hodinu. V Amerike tento typ útoku stál firmy 5 miliárd dolárov ročne. Štatistika spoločnosti Shape Security hovorí, že 60% prihlásení v leteckom a bankovom sektore spadá pod škodlivé pokusy. V hotelierstve je to 44% a v obchodnom sektore neuveriteľných 91%. Našťastie existuje pozitívny trend implementovať silnejšiu viacfaktorovú autentifikáciu. Na bezpečnosť aplikácií však treba dbať najmä ak si na ich vývoj prenajímate služby programátora freelancera.

Ďalším druhom útoku, ktorý v minulom roku významne vzrástol je tzv. „formjacking“. Útočníci zneužijú ukradnuté prihlasovacie údaje, alebo zraniteľnosti použitých knižníc od tretích strán a injektujú jednoduchý Javascript kód na webstránku online obchodu a ten prečíta údaje z kreditnej karty, ktoré zákazník zadá do formuláru pri platbe. Významným činiteľom v tejto oblasti sú skupiny využívajúce rôzne verzie skriptu MageCart. Správa spoločnosti Symantec hovorí, že v minulom roku spoločnosť zachytila 3,7 milióna pokusov o formjacking. Ukradnuté platobné údaje môžu útočníci zneužiť priamo, alebo ich predať na darkwebe, pričom za jednu kreditku môžu dostať aj 45 USD.

Ako je možné, že dochádza k takýmto katastrofálnym únikom citlivých údajov?

Správa spoločnosti Positive Technologies hodnotiaca jej aktivity v oblasti penetračného testovania v roku 2018 hovorí, že testeri úspešne prenikli do vnútorných sietí až 92% testovaných inštitúcií. Najvýhodnejším vektorom útoku boli nechránené zraniteľné webové aplikácie vystavené dovonku. Testerom umožnili prístup k vnútornej sieti až v troch štvrtinách úspešných prípadov. Ku zvýšeniu

práv a prístupu ku kritickým systémom veľmi úspešne využívali základné techniky vrátane zneužívania starých neopravených zraniteľností, zraniteľností na wi-fi sieťach a lámanie prístupových hesiel hrubou silou.

Zraniteľnosti systémov, ktoré sa môžu stať spoločnosti osudné, sa objavujú na dennom poriadku, a preto je potrebné mať vhodný plán aktualizácií softvéru. Správa spoločnosti Risk Based Security hovorí, že v roku 2018 bolo odhalených vyše 22 000 zraniteľností, z ktorých takmer polovica bola spojená s webovými aplikáciami. Tretina z celkového počtu bola označená ako závažná a kritická. Pritom vyše štvrtina odhalených zraniteľností ostala bez opravných aktualizácií. Odhaľovaniu zraniteľností významne pomáhajú odmeňovacie programy, akým je napríklad európsky projekt FOSSA zameraný na 14 často používaných open-source projektov (Drupal, Filezilla, Apache Tomcat, PuTTY, VLC, ...) s rozpočtom na odmeny takmer milión eur.

Mnohé spoločnosti si uvedomujú, že sa nedokážu efektívne chrániť pred prienikom zvonku. Štúdia spoločnosti Ponemon dotazujúca až 600 bezpečnostných expertov z komerčného sektoru hovorí, že toto presvedčenie zdieľa až 44% z nich. Zároveň viac ako 2/3 sa vyjadrili, že nemajú dostatok času a prostriedkov, aby sa zaoberali všetkými zraniteľnosťami zneužiteľnými pre prístup k citlivým dátam spoločnosti, pre ktorú pracujú. Skúseným útočníkom pritom na prienik stačí priemerne len niekoľko hodín; najlepším len 20 minút.

Jedným z možných riešení, ktoré citeľne zvýšia bezpečnosť vašich dát, je využívanie virtuálnych privátnych sietí – VPN. Sú to akési šifrované tunely, cez ktoré môžu bezpečne tiecť dáta. Ak sa pre rozhodnete pre VPN, používajte ju na všetkých zariadeniach, celý čas a dbajte na správnu konfiguráciu, aby vaši zamestnanci necítili obmedzenie funkčnosti internetového pripojenia. To by ich mohlo lákať VPN vypnúť. Taktiež majte pod kontrolou, aké dáta vašim tunelom tečú. Stačí totiž jeden infikovaný počítač a aj napriek VPN môže byť ohrozená celá sieť.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci marec riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Okrem toho pokračoval v riešení incidentu a nachádzaní nových zraniteľností v systéme eID. Riešil tiež únik dát z e-mailovej schránky zamestnanca jednej inštitúcie, ktorý nastal po tom, ako zamestnanec klikol na odkaz vo phishingovom e-maile.

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

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

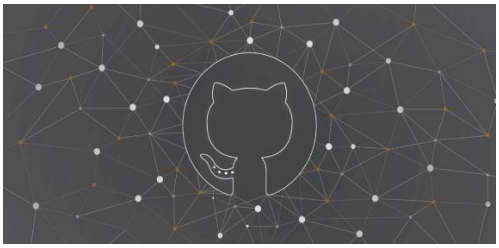
CSIRT.SK sa tiež venoval príprave novej vyhlášky Úradu podpredsedu vlády SR pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.

Významné útoky vo svete

Útoky na routre Cisco RV110, RV130 a RV215 začali dva dni po vydaní aktualizácií

Kritická zraniteľnosť v routeroch pre malé spoločnosti a domácnosti od spoločnosti Cisco, vďaka ktorej dokážu útočníci jednoduchým spôsobom ovládnuť router na diaľku z internetu, sa stala populárnou medzi útočníkmi dva dni po vydaní aktualizácie a deň po vydaní funkčnej ukážky jej zneužitia. Túto ukážku kódu zvyknú útočníci využívať pri svojej škodlivej aktivite. Spoločnosť Bad Packets zaznamenala skenovanie internetu za účelom vyhľadať zraniteľné zariadenia. Zraniteľné sú wifi routery RV110, RV130 a RV 215. Vzhľadom na ich cieľovú skupinu ostane veľa kusov dlhú dobu bez opravy.

89 účtov na GitHube šírilo vyše 300 aplikácií s vytvorenými zadnými vrátkami



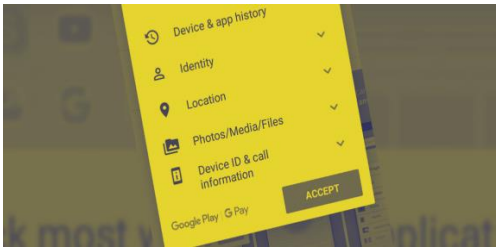
305 upravených legitímnych aplikácií s vloženými zadnými vrátkami bolo hostovaných na repozitároch GitHub. Do kampane bolo zapojených 89 škodlivých účtov, z ktorých mnohé slúžili na zvýšenie popularity škodlivých aplikácií vo vyhľadávaní GitHubu. Škodlivé verzie aplikácií vytvárali na systémoch obetí perzistenciu a neskôr sťahovali ďalší malvér, ktorý napríklad zapájal zariadenia do botnetu. Všetky škodlivé účty boli z GitHubu odstránené.

18 verejne dostupných MongoDB databáz sprístupňuje osobné údaje stoviek miliónov čínskych občanov

Bezpečnostný výskumník Victor Gevers našiel z internetu prístupné databázy zbierajúce údaje zo 6 čínskych sociálnych sietí. Tieto údaje vrátane rozhovorov boli priradené konkrétnym osobám, alebo ich identifikačným prvkom, čo sa týkalo 364 miliónov profilov. Monitorované údaje boli odoslané lokálnym policajným autoritám v prípade, keď systém zaznamenal špecificky zaujímavé dáta. Vzhľadom na objem ukladaných citlivých dát je zarážajúce, že tento sledovací systém postrádal akékoľvek zabezpečenie a bol dostupný komukoľvek cez internet.

TLP: White

Vyše polovica z 81 VPN aplikácií pre Android požaduje prístup k citlivým údajom



John Mason zo spoločnosti TheBestVPN.com urobil analýzu povolení, ktoré vyžadovalo 81 aplikácií pre Android poskytujúcich anonymizačnú službu VPN. 50 z nich vyžadovali aspoň jedno povolenie pre prístup k osobným údajom, pre ktoré nemali opodstatnené využitie. VPN aplikáciám by mal postačovať prístup INTERNET a ACCESS_NETWORK_STATE. Väčšina však vyžadovala aj ďalšie, napríklad prístup na čítanie a zapisovanie na externé úložisko, k lokálnym súborom, lokalizačným dátam, čítaniu a zmene systémových nastavení, či logom.

Útoky smerované cez herné aplikácie na deti

Spoločnosť Rubica vydala správu, v ktorej analyzuje bezpečnosť zadarmo poskytovaných herných aplikácií pre deti mladšie ako 12 rokov. Takéto aplikácie často obsahujú agresívnu reklamu a návrhy na inštaláciu dodatočných aplikácií, čo mladšie deti ešte nevedia kriticky zhodnotiť a môžu sa tak ľahko stať obeťami útočníkov. Ponúkané aplikácie často umožňujú útočníkom získať prístup k zariadeniu vrátane emailových účtov a bankových aplikácií. Správa hovorí, že existuje veľké množstvo nezverejnených prípadov obetí, ktoré prišli o nemalé finančné čiastky práve týmto spôsobom.

Za minulý rok zažilo útok bankovým malvérom 1,8 milióna používateľov Android zariadení

Najviac obetí útokov bankovým malvérom v roku 2018 pochádzalo z Ruska, USA a Juhoafrickej republiky. 85% útokov využilo malvér Asacub, Agent, alebo Svpeng. Spoločnosť Kaspersky Lab zaznamenala v roku 2018 116,5 milióna útokov na mobilné zariadenia, využívajúcich škodlivý kód. To predstavuje takmer dvojnásobok oproti roku 2017. Útočníci využili overený SMS spam, no tiež iné metódy, ako DNS hijacking.

Pokusy infikovať malvérom hráčov cez zraniteľnosti v hernom klientovi zaznamenané u 39% herných serverov Counter Strike 1.6

Až 39% herných serverov populárnej hry Counter Strike 1.6 bolo na vrchole botnetu odhaleného spoločnosťou Dr. Web škodlivých so zámerom infikovať trójskym koňom Belonard svoje obete. Tieto boli zapojené do botnetu. Trójsky kôň využíval na svoje šírenie zraniteľnosti v hernom klientovi, alebo škodlivú verziu tohto klienta. Dr. Web v spolupráci s REG.ru odstavili domény, ktoré malvér používal na presmerovanie obetí na falošné herné serveri. To by spolu s využitím tzv. sinkhole serverov malo zabrániť jeho opätovnému šíreniu.

Európska Únia má nový protokol pre reakciu na závažné kybernetické incidenty presahujúce hranice jedného štátu

EÚ má nový protokol na riešenie závažných kybernetických incidentov s väčším rozsahom dopadu, Law Enforcement Emergency Response Protocol. Implementovaný bude Europolom, konkrétne útvarom European Cybercrime Centre (EC3). Sústredí sa na rýchlu analýzu, zdieľanie informácií a koordináciu medzinárodného vyšetrovania. Využívaný bude pri riešení kriminálnej a zámere škodlivej kybernetickej činnosti.

Nórsky gigant zasiahnutý kyberútokom – producent hliníku Norsk Hydro napadnutá ransomvérom LockerGoga

Nórsky hliníkový gigant Norsk Hydro, operujúci v 50 krajinách sveta, sa stal obeťou útoku ransomvérom a niektoré prevádzky tak museli prejsť na manuálnu operáciu. Spoločnosť sa vyjadrila, že situácia je vážna a nefunguje sieťové spojenie prevádzok po celom svete. To zapríčinilo problémy s výrobou a pozastavenie prevádzky v niektorých výrobniach. Vyšetrovanie odhalilo, že útočníci použili ransomvér LockerGoga a infekcia sa začala šíriť pravdepodobne z USA. Spoločnosť nezaplatila výkupné a obnovila svoje systémy zo záloh.

FBI zrušila 15 najväčších svetových domén poskytujúcich nájom DDoS útokov. 85% pokles DDoS útokov.

Americká FBI sa minulý rok zamerala na webové stránky ponúkajúce služby DDoS útokov. Zaistila 15 najväčších svetových domén. Počet útokov tak koncom minulého roka klesol v porovnaní s koncom roka 2017 o 11%. Priemerné objemy DDoS útokov klesli o 85% a maximálne o 24%. Zároveň sa problematikou DDoS útokov v roku 2018 zaoberal aj Europol, pričom okrem iného sa mu podarilo zrušiť službu WebStresser. DDoS útoky v Európe následne poklesli o 60%.

Austrálski kyber-bojovníci proti Islamskému Štátu

Riaditeľ Australian Signals Directorate v príhovore k Lowy Institute v Sydney uviedol, že jeho útvar viedol úspešnú kybernetickú kampaň na podporu koaličných síl bojujúcich v Sýrii proti Islamskému štátu. Počas ofenzívy proti pozíciám IS v roku 2016 austrálski hackeri zaútočili na komunikačné kanály veliteľov teroristov zo svojej domoviny a znemožnili jednotlivým skupinám počas útoku spojencov komunikovať. ASD spolupracovala aj pri ďalších protiteroristických a výzvedných operáciách s vysokou efektivitou.

- **Botnet Necurs začal využívať techniky na krytie svojej aktivity a šíri nový malvér**
- **Oznámenie znásobenia množstva phishingových útokov na hedgeové fondy a finančné inštitúcie**
- **Nové dôkazy spájajúce kyber-špionážnu kampaň Sharpshooter so severokórejskou APT Lazarus**
- **Rekordne vysoká pokuta pre TikTok za zber dát detí mladších ako 13 rokov**
- **Zdravotnému systému Rush unikli osobné dáta 45 000 pacientov**
- **Osobné údaje 5 miliónov občanov Saudskej Arábie dostupné cez nezabezpečenú MongoDB databázu patriacu aplikácii Dalil, identifikujúcej volajúcich**
- **Čínski útočníci viedli výzvednú kampaň voči prominentným americkým univerzitám s cieľom získať informácie o vojenských technológiách**

TLP: White

- Predaju SSL/TLS certifikátov na Darkwebe sa darí
- Voľne dostupná databáza MongoDB s vyše 800 miliónmi záznamov
- Prienik do internej siete spoločnosti Citrix a krádež 6TB firemných dokumentov má na svedomí pravdepodobne Irán
- Okres Jackson County v Georgii zaplatil 400 000 dolárov útočníkom na dešifrovanie svojich dát po ransomvérovom útoku
- Hlasový phishing v USA vzrástol 20-násobne, podvodníci sa vydávajú za pracovníkov daňového úradu
- Facebook žaluje dvoch Ukrajincov, ktorí pomocou kvízových aplikácií presvedčili užívateľov, aby si stiahli do svojho prehliadača ich modul. Zozbierali osobné údaje 63 000 používateľov.
- Nezabezpečená čínska Elasticsearch databáza exponovala údaje 33 miliónov uchádzačov o prácu
- Dve tretiny antivírusových aplikácií pre Android nefungujú tak, ako by mali. Niektoré ani neskenujú sťahované a inštalované aplikácie.
- Nezabezpečená databáza s osobnými údajmi singapurských darcov krvi ponechaná internetu
- Ďalšia nezabezpečená Elasticsearch databáza – e-shopu Gearbest – odhaľovala citlivé údaje 1,5 milióna zákazníkov, vrátane prihlasovacích údajov
- Z internetu dostupná Elasticsearch databáza obsahujúca vyše 257 000 právnych dokumentov
- K minulomesačnému úniku údajov k účtom stoviek miliónov používateľov pridal zodpovedný aktér na darkweb ďalších 26 miliónov zo šiestich webstránok
- Litovčan podvodom získal od Googlu a Facebooku 123 miliónov dolárov, hrozí mu 30 rokov vo väzbe.
- Internetové obchody MyPillow a Amerisleep napadnuté kódom Magecart na krádež údajov z platobných kariet
- Facebook mal roky heslá používateľov uložené vo voľnom texte. Dostupné boli pre 20 000 zamestnancov.
- Úspešný spear phishingový útok na účty zamestnancov oregonského Department

of Human Services exponoval 2 milióny citlivých e-mailových správ od vyše 350 000 občanov

- Denne dochádza k úniku tisícok API a kryptografických kľúčov na GitHube
- Americké chemické firmy Hexion a Momentive tiež obeťou útoku ransomvérom LockerGoga
- Americká agentúra FEMA zdieľala zbytočne veľa citlivých dát 2,3 milióna preživších obetí prírodných katastrof. Vrátane bankových údajov.
- Niektoré predinštalované aplikácie na smartfónoch zbierajú a odosielajú dáta o používateľoch
- Microsoft zabavil 99 domén využívaných na útoky iránskou skupinou APT35
- Prienik do systému kanadskej inštitúcie Natural Health Services spôsobil únik osobných informácií 34 000 používateľom medicínskej marihuany
- Prienik do systému spoločnosti Toyota a krádež údajov 3,1 milióna vlastníkov automobilov Toyota a Lexus

Závažné zraniteľnosti bežných softvérových produktov

Aktívne zneužívaná zero-day zraniteľnosť v prehliadači Google Chrome

Kritická zraniteľnosť v prehliadači Google Chrome typu "Use after free" (použitie odalokovaného miesta v pamäti) umožňuje vzdialene vykonávať kód v systéme obete a prevziať tak kontrolu nad jej zariadením. Zraniteľnosť je aktívne zneužívaná a spoločnosť Google na ňu nedávno vydala opravu. Odporúča sa bezodkladne aktualizovať prehliadač Chrome.

Kritická zraniteľnosť v balíkoch Pacman

Bola nájdená kritická zraniteľnosť CVE-2019-9686 v manažéri softvérových balíčkov Pacman. Zraniteľnosť umožňuje vykonávanie škodlivého kódu ak si používateľ inštaluje balík zo špeciálnej URL adresy. Ide o útok man-in-the-middle.

Kritická zraniteľnosť WordPress umožňuje ľahko ovládnuť webstránku cez komentáre

Zraniteľnosť v Content Management Software (CMS) WordPress môže viesť ku vzdialenému vykonávaniu kódu. Zraniteľnosť vzniká pri chybných cross-site požiadavkách (CSRF) v časti pre komentáre v programe WordPress. Táto časť programu je jednou zo základných súčastí, ktorá je štandardne povolená a ovplyvňuje všetky inštalácie programu WordPress pred verziou 5.1.1. Daná zraniteľnosť dokonca umožňuje neautentifikovanému vzdialenému útočníkovi, aby kompromitoval systém a vzdialene vykonával kód na zraniteľných webových stránkach.

Aktívne zneužívaná 19-ročná kritická zraniteľnosť vo WinRARe

V aplikácii na kompresiu dát WinRAR bola opravená kritická zraniteľnosť umožňujúca útočníkom vzdialene vykonávať kód. Zraniteľné sú všetky verzie vydané za posledných 19 rokov pred opravnou aktualizáciou 5.70 beta 1. V prvom týždni po zverejnení zraniteľnosti bolo zaznamenaných vyše 100 rôznych kampaní, v ktorých bola zneužívaná. Nakoľko WinRAR nepodporuje automatické aktualizácie, používatelia si musia novú verziu nainštalovať manuálne.

TLP: White

PuTTY opravilo 8 vysoko závažných zraniteľností

Klient PuTTY pre pripojenie pomocou protokolov SSH, Rlogin a Telnet, obsahoval osem vysoko závažných zraniteľností. Ich zneužitím mohol útočník spôsobiť nedostupnosť systému, vzdialene vykonávať kód, či získať prihlasovacie údaje. Bola vydaná opravná aktualizácia.

Kombinovaná zero-day zraniteľnosť vo WordPress doplnku Social Warfare

WordPress doplnok Social Warfare obsahuje kritickú zero-day zraniteľnosť umožňujúcu vykonávať XSS útoky a vzdialene vykonávať kód na zraniteľnej webstránke a v prehliadači obete, ktorá na kompromitovanú stránku pristúpi. Zraniteľnosť je aktívne zneužívaná a postihuje desiatky tisíc stránok. Útočníkovi dovoľuje prevziať kontrolu nad zraniteľnou webstránkou, aj prehliadačom obete. Odporúča sa bezodkladná aktualizácia.

Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Enterprise Chat and Email (CVE-2019-1702): nedostatočná sanitizácia používateľského vstupu do webového manažérskeho rozhrania spôsobuje niekoľko XSS zraniteľností.
Cisco Common Services Platform Collector (CVE-2019-1723): Cisco Elastic Services Controller obsahuje prednastavený účet so statickými prihlasovacími údajmi, čo môže byť zneužité na obídenie autentifikácie.
Cisco IP Phone 8800 Series (CVE-2019-1763): kvôli nesprávnej sanitizácii URL adries z požiadaviek je možné získať neoprávnený prístup do webového manažovacieho rozhrania SIP softvéru.
Cisco IOS a IOS XE (CVE-2019-1723, CVE-2019-1738, CVE-2019-1739, CVE-2019-1740): zraniteľnosti pri narábaní s paketmi umožňujú vyvolať DoS podmienky.
Cisco IOS (CVE-2019-1751): pri narábaní so špeciálne upravenými IPv4 paketmi nastáva v NAT64 možnosť vytvoriť DoS podmienky.
Cisco IOS XE (CVE-2019-1742, CVE-2019-1743, CVE-2019-1745): nesprávna kontrola prístupov k súborom a užívateľských vstupov cez webové rozhranie umožňuje lokálne injektovanie príkazov, únik informácií a neautorizované nahrávanie súborov.
Cisco IOS XE Software (CVE-2019-1753, CVE-2019-1754, CVE-2019-1755, CVE-2019-1756): vzdialené zvýšenie práv je umožnené nesprávnym sanitizovaním vstupov vo funkciách Web Services Management Agent a vo webovom rozhraní. To tiež umožňuje injektovať príkazy.

TLP: White

Cisco Catalyst 4500 Series Switches (CVE-2019-1750): nevhodné spracovávanie chýb pri spracovávaní CDP paketov umožňuje vytvoriť DoS podmienky.

VMware

V produktoch VMware bolo opravených viacero rozličných kritických a závažných zraniteľností:
VMware Workstation Pro / Player (CVE-2019-5511/5512): chyba umožňujúca eskaláciu práv. Vzniká nesprávnym narábaním s cestami a umožňuje prístup k súboru VMX.
VMware Workstation: kvôli súbehu a zápisu mimo povolené hranice pamäte je možné vzdialene vykonávať kód v kontexte zraniteľnej aplikácie.
VMware ESXi, Workstation and Fusion (CVE-2019-5514, CVE-2019-5515, CVE-2019-5518, CVE-2019-5519, CVE-2019-5524): väčšinou chyby zápisu do pamäte mimo povolený rozsah a tiež voľne dostupná API cez webové rozhranie. Útočníkovi umožňujú vykonávať kód a spúšťať príkazy na hostiteľskom a hosťovskom systéme.
VMware vCloud Director for Service Providers (CVE-2019-5523): zraniteľnosť umožňuje útočníkovi pristúpiť a prevziať kontrolu nad bežiacou reláciou a ristupovať k portálom Tenant a Provider.

Microsoft Azure

V cloudovom produkte Microsoft Azure bolo opravených viacero rozličných kritických a závažných zraniteľností:
Microsoft Azure SSH Keypairs (CVE-2019-0816): chyba umožňuje obísť zabezpečenie systému a pridávať cudzie verejné kľúče do súboru autorizovaných kľúčov na virtuálnom systéme. Toto je možné, ak útočník pristupuje k službe zo systému Ubuntu Linux.
Microsoft Azure Linux Guest Agent (CVE-2019-0804): spôsob, akým Azure WaLinuxAgent vytvára swapovacie súbory na diskoch, umožňuje únik informácií.

Mesačník zraniteľností Marec 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
    - WinRAR
    - CMS WordPress
    - Manažér softvérových balíčkov Pacman pre Linux

https://www.csirt.gov.sk/aktualne-7d7.html?id=183