MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK
Júl 2020

Vypracoval: CSIRT.SK

TLP: White

Pravdepodobne najsledovanejším kybernetickým útokom na svete za posledné mesiace je útok na používateľské účty na platforme Twitter. V stredu 15. júla 2020 získali neznámi útočníci na portáli Twitter kontrolu nad 130 kontami. Cieľom boli kontá veľkých spoločností a známych osobností, ako napríklad @Apple, @Bitcoin, @BarackObama, @JeffBezos, @elon_musk, @BillGates, @WarrenBuffett. Na týchto kontách následne útočníci propagovali podvodnú schému. Účty celebrít zverejňovali jeden po druhom tú istú zvláštnu správu: Pošlite bitcoiny a my vám pošleme dvojnásobok vašich peňazí. Útočníci takto získali bitcoiny v hodnote viac ako 120 000 dolárov v priebehu približne 3 hodín. Ďalších 280 000 dolárov nebolo poslaných vďaka spoločnosti Coinbase, ktorá zablokovala transakcie na bitcoinové peňaženky u svojich klientov už v prvých minútach útoku. Krátko nato Twitter zablokoval tieto kontá a zresetoval ich heslá. Po vyšetrovaní spoločnosť oznámila, že útočníci získali prístup na interné administratívne nástroje po tom, čo získali prihlasovacie údaje zamestnancov Twitteru pomocou sociálneho inžinierstva. Na kontá sa dostali tým, že použili reset hesla. Samotné heslá teda neunikli. Okrem toho Twitter priznal, že útočníci čítali súkromné správy na minimálne 36 kontách.

Zatiaľ čo niektorí spočiatku považovali útok za prácu pokročilých útočníkov, ukázalo sa, že „mastermind“ jedného z najvýznamnejších útokov za posledné roky bol 17-ročný absolvent strednej školy na Floride. Graham Ivan Clark bol zatknutý vo svojom byte v Tampe, kde mu bolo oznámené, že čelí 30 obvineniam z ťažkých zločinov, vrátane podvodov, a že bude súdený ako dospelý. Dvaja ďalší útočníci Mason John Sheppard (19) a Nima Fazeli (22) z Orlanda, boli obvinení z pomoci Clarkovi počas útoku. Prokuratúra uviedla, že sa zdá, že obaja pomáhali ústrednej osobe útoku, ktorá sa volala Kirk. Zverejnené informácie neposkytujú skutočnú totožnosť Kirka, no naznačujú, že to bol Clark.

Osoba nazývaná Kirk bola objavená na online chatovacej platforme Discord. 15. júla 2020 používateľ s prezývkou Kirk na platforme Discord predložil lákavú ponuku. V správe uviedol, že pracuje pre Twitter a že je schopný prebrať účet s akýmkoľvek menom, samozrejme za finančnú odmenu. Táto ponuka bola lákadlom pre mnohých, prevažne hráčov či iných používateľov Twitteru, ktorí sú ochotní zaplatiť nemalé peniaze za to, že dostanú prihlasovacie údaje k účtom s nezvyčajnými používateľskými menami. Takéto mená sa zvyknú nazývať aj „OG user names“ a sú nimi napríklad jednopísmenkové účty, účty s názvom obsahujúcim len jedno slovo (napríklad @bumblebee) alebo jedno číslo. K takýmto účtom sa zvyčajne na platformách dostanú tí, ktorí sú ich prvými návštevníkmi.

Napriek tomu čo Kirk tvrdil v správe na Discord, nebolo pravdou, že je zamestnancom spoločnosti Twitter. Toho istého rána niekto na fóre OGUsers začal pod menom Chaewon ponúkať prístup k akémukoľvek účtu na Twitteri. Ceny za jeden takýto účet sa pohybovali približne v rozmedzí od 2500$ do 5000$. Na Discorde takisto prebehla komunikácia medzi používateľmi Kirk a Rolex, kde Kirk aby dokázal svoje schopnosti, zmenil priradený email z účtu @foreign na email používateľa Rolex.

FBI verí, že používateľ Rolex je v skutočnosti Fazeli, a obvinila ho z napomáhania a podnecovania k neoprávnenému prístupu k chránenému počítaču. Hrozí mu 5 rokov väzenia a pokuta vo výške

250 000$. FBI tiež tvrdí, že používateľ Chaewon je v skutočnosti Sheppard, ktorý je obvinený zo sprisahania s cieľom spáchať podvod, zo sprisahania za účelom prania špinavých peňazí a z neoprávneného prístupu k chránenému počítaču. Hrozí mu 45 rokov väzenia a pokuta vo výške 750 000$. K účtom na Twitteri sa Clark dostal pomocou phishingu. Údajne presvedčil jedného zo zamestnancov spoločnosti, že je spolupracovníkom v technologickom oddelení, ktorý potreboval poverenia zamestnanca na prístup na portál služieb zákazníkom.

17-ročný Clark sa momentálne nachádza vo väzení s kauciou 725 000$. Jeho obhajca David Weisbrod podal návrh, ktorého cieľom bolo znížiť kauciu jeho klienta a zrušiť rozhodnutie súdu, že Clark musí preukázať, že všetky prostriedky použité na odoslanie kaucie boli získané legitímne. Weisbrod tvrdí, že kaucia je neprimeraná a že tvorí 6-násobok sumy, za ktorej krádež je Clark obvinený. Preukázanie neviny je náročné najmä preto, že Clark už v minulosti bol stíhaný za takýto typ priestupkov. V reakcii na návrh Weisbrodovej redukcie kaucie sa štátny zástupca Darrell Dirks vyjadril, aby sa zachovalo ustanovenie, podľa ktorého musí Clark preukázať legitimitu svojich finančných prostriedkov. Tvrdil, že minulý rok bol Clark predmetom federálneho a kalifornského vyšetrovania údajnej krádeže kryptomeny obetí v Kalifornii v hodnote asi 1 milión dolárov. Clark súhlasil so zaplatením kryptomeny v hodnote 900 000 dolárov ako „čiastočné vrátenie peňazí“ obetiam Kalifornie. V tej dobe mal Clark iba 16 rokov.

Dirks tiež uviedol, že kaucia vo výške 725 000$ bola primeraná, pretože straty v prípade sa nemusia nevyhnutne obmedzovať na 117 000$. Sudca vystúpil s ustanovením, že Clark musí preukázať, že legitímne získal prostriedky, ktoré používa na zloženie kaucie a že táto kaucia sa nebude znižovať.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci júl riešil štandardne najmä phishingové kampane na svoju konštituenciu a informoval o zraniteľnostiach systémov.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK rozposlala svojej konštituencii varovanie pred kritickou zraniteľnosťou produktov F5 BIG-IP, umožňujúcou kompromitáciu infraštruktúry. Konštituencia bola priamo informovaná aj o kritickej zraniteľnosti CVE-2020-1350 vyskytujúcej sa v systémoch Windows Server, ktorá útočníkom umožňuje prevziať kontrolu nad DNS serverom, a teda nad celým informačným tokom organizácie.
Varovala tiež pred kampaňou šíriacou ransomvér Sodinokibi / REvil, ku ktorej poskytla indikátory kompromitácie (IoC) v podobe IP adries C&C serverov. Varovanie bolo rozposlané aj ohľadom kampane ruskej skupiny APT 29, ktorá zneužívala štyri zraniteľnosti produktov Citrix, Pulse Secure, FortiGate a Zimbra vo svojej kampani zameranej na krádež informácií z vývoja vakcíny proti vírusu Covid-19. Jednotka rozposlala tiež varovanie s IoC na phishingovú kampaň, cielenú na produkt Microsoft Office 365, o ktorej informoval NBÚ. Na trhu IT produktov boli odhalené tiež falošné verzie zariadení Cisco WS-2960X, o čom bola konštituencia CSIRT.SK informovaná.

Významné útoky vo svete

Útoky na databázy MongoDB využívajú GDPR ako prostriedok na vydieranie

Útočníci sa zamerali na nezabezpečené servery MongoDB a mažú ich databázy. Na skoro 23 tisícoch serverov zanechali správy požadujúce výkupné. Napadnuté databázy tvoria skoro 47 percent zo všetkých MongoDB databáz a neboli chránené heslom. Na vyhľadávanie nesprávne nakonfigurovaných databáz využívajú útočníci automatizovaný skript. Požadujú vyplatenie výkupného 0,015 bitcoinov počas 2 dní od útoku, inak hrozia únikom údajov a kontaktovaním miestnych orgánov ohľadom zákona o ochrane osobných údajov (GDPR).

Malvér pre Windows posielal informácie o kreditných kartách cez DNS záznamy

Malvér Alina sa špecializuje na platiace systémy a monitoruje ich s cieľom zachytiť platby kreditnou kartou. Pri spracovaní platby malvér odchytí informácie o karte z pamäte stroja a odošle ich na server útočníka. Z týchto údajov môže útočník urobiť kópiu karty, využiť ich na nákupy alebo ďalej predať. Takéto systémy ale bývajú zabezpečené a často je povolená len komunikácia nevyhnutná na prevádzku. Medzi blokované protokoly patrí aj http, ktorý sa bežne využíva pre komunikáciu so servermi. DNS protokol je ale často povolený, preto bol využitý na útok. Zakódované informácie o kreditných kartách sa posielali vo forme poddomény v DNS požiadavke.

APT15 má väzby na čínsku vojenskú spoločnosť

Bezpečnostná spoločnosť Lookout vydala správu dokazujúcu, že čínska hackerská skupina APT15 má väzby na čínskeho vojenského dodávateľa. Bezpečnostní špecialisti našli počas výskumu tejto skupiny nechránený kontrolný server pre nový špionážny malvér GoldenEagle. Ten je využívaný na sledovanie národnostných menšín. Bezpečnostným špecialistom sa podarilo získať informácie o obetiach daného malvéru. Podľa týchto informácii úplne prvé obete pravdepodobne slúžili ako testovacie zariadenia pri vývoji škodlivého kódu.

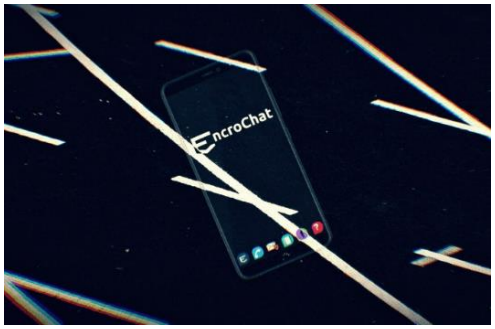
Nová verzia ransomvéru Snake/EKANS obsahuje nové funkcionality

Ransomvér Snake sa špecializuje na kontrolné systémy veľkých industriálnych spoločností. V júni bol použitý v útoku proti spoločnosti Honda. Bezpečnostní výskumníci z FortiGuard Labs získali vzorku tohto malvéru. Z jej analýzy zistili, že malvér si vyberá svoju obeť, a ak nie je v cieľovej sieti, ukončí sa. Pravdepodobne sa snaží aj o detekciu antivírusových programov. Okrem toho je Snake schopný využiť a modifikovať firewall pridávaním nových pravidiel na blokovanie nechcenej prevádzky. Ransomvér ukončí preddefinované procesy, aby sa informácie, ktoré uchovávali uložili a mohol ich zašifrovať.

Výrobca smart hodiniek Garmin mal výpadok spôsobený ransomvérom

Výrobca smart hodiniek, fitness a GPS doplnkov Garmin bol napadnutý ransomvérom WastedLocker, ktorý patrí skupine Evil Corp. Zašifrovanie dát spôsobilo štvordňový výpadok služieb spoločnosti. Spoločnosť odmietla komentovať výšku výkupného a to, či zaplatila. Zamestnanec spoločnosti kontaktoval BleepingComputer a tvrdil, že výkupné malo byť 10 miliónov dolárov. Okrem toho získali dekryptor s dešifrovacím kľúčom, ktorý mal byť použitý pri dešifrovaní dát Garminu. Z toho vyplýva, že spoločnosť výkupné zaplatila.

Európske policajné zložky zatkli stovky ľudí po tom, čo prenikli do šifrovanej siete



Spoločnosť EncroChat predávala mobilné telefóny s modifikovaným systémom Android s hardvérovým šifrovaním a predinštalovanou šifrovanou chatovacou aplikáciou z ktorej bolo možné vymazať všetky dáta aj na diaľku. Túto aplikáciu často využívali skupiny organizovaného zločinu. Preto európske orgány činné v trestnom konaní vytvorili vyšetrovací tím, ktorého cieľom bolo monitorovať ju. Tímu sa podarilo infiltrovať platformu, obísť šifrovanie a monitorovať milióny správ. Skupina stojaca za EncroChat ale zistila, že v ich telefónoch je malvér a že ich doména bola infiltrovaná. Varovali o tom všetkých používateľov a vypli svoje servery. Napriek skorému prerušeniu operácie sa však podarilo zatknúť stovky podozrivých vo viacerých krajinách Európy. Okrem toho sa polícii vďaka správam podarilo prekaziť množstvo kriminálnych operácií vrátane nájomných vrážd.

62 tisíc QNAP NAS zariadení bolo infikovaných malvérom QSnatch

Bezpečnostné agentúry zo Spojených štátov amerických a Veľkej Británie vydali varovanie pre používateľov NAS zariadení od spoločnosti QNAP. Vyzývali používateľov, aby aktualizovali svoje zariadenia. Okrem toho odporúčajú pred aktualizáciou reset zariadení, ktoré stále používajú zraniteľné verzie, keďže tento malvér dokáže blokovať inštaláciu aktualizácií. Bolo nájdených 62 tisíc zariadení infikovaných malvérom QSnap. Ten dokáže zachytiť prihlasovacie údaje, vytvoriť falošnú prihlasovaciu stránku na zariadení, otvoriť prístup pre vykonávanie vzdialeného kódu a kradnúť údaje. Súčasne boli identifikované dve predošlé kampane – jedna medzi rokmi 2014 a 2017, druhá medzi 2018 a 2019. V poslednej kampani si malvér generoval domény, cez ktoré komunikoval s riadiacim serverom.

Severná Kórea je spojená s útokmi na obchody v USA a Európe

Výskumníci z holandskej spoločnosti Sansec zistili, že pri útokoch MageCart na obchodné reťazce v Európe a USA za posledný rok bola použitá infraštruktúra útočnej skupiny Lazarus zo Severnej Kórei. MageCart útoky zahŕňajú kradnutie informácií o kreditných kartách skenovaním platobných stránok online obchodov. Útočníci kompromitovali viaceré legitímne stránky a využili ich ako medzičlánok, cez ktorý posielali informácie o kreditných kartách, aby zakryli stopy ku svojim serverom. Okrem toho si registrovali domény podobné doménam obetí ktoré tiež využívali na prenos dát.

Útočníci požadovali od spoločnosti EDPR NA 10 miliónov za dešifrovanie dát

Spoločnosť EDP Renewables North America ktorá je dcérskou spoločnosťou Portugalskej korporácie Energias de Portugal (EDP) potvrdila ransomvérový útok na EDP. Útočníci získali 10 TB dát a požadovali 1580 bitcoinov, čo je viac ako 10 miliónov dolárov, za dešifrovanie a to, že údaje nezverejnia. Neskôr v máji vyšetrovanie ukázalo, že EDPR NA utrpela stratu dát po tom, čo sa útočníci dostali do jej siete. Útočníci sa nemali dostať k žiadnym osobným informáciám, aj keď spoločnosť stále útok prešetruje. Napriek tomu spoločnosť vyzýva svojich klientov k zvýšenej opatrnosti, keďže databáze má uložené osobné informácie klientov vrátane Social Security čísla a mien.

Bankový Trojan Cerberus sa šíril cez aplikáciu na Google Play

Cerberus je pokročilý bankový trójsky kôň ktorý má širokú funkcionalitu vrátane spúšťania aplikácií, napodobňovania bankových notifikácií, extrahovania kódov pre dvojfaktorovú autentifikáciu a zachytávania písaného textu. Pri zapnutí bankovej aplikácie prekryje jej okno a používateľ zadá prihlasovacie údaje do Cerbera. Trojan sa skrýval za aplikáciu na konverziu meny „Calculadora de Moneda“ ktorá bola dostupná na Google Play od marca. Prvých niekoľko týždňov fungoval ako legitímna aplikácia aby sa vyhol detekcii skôr ako sa rozšíri. Od polovice júna už aplikácia obsahovala kód na stiahnutie samotného malvéru, ktorý ešte nebol aktivovaný. Od 1. - 6. júla sa aplikácia pripojila na riadiaci server a stiahla Cerberus. Po tomto kroku aplikácia už nesťahuje malvér a funguje ako legitímna aplikácia. Spoločnosť Google sa k situácii nevyjadrila.

V čínskom daňovom softvéri sa nachádzal nový malvér

Trustwave®

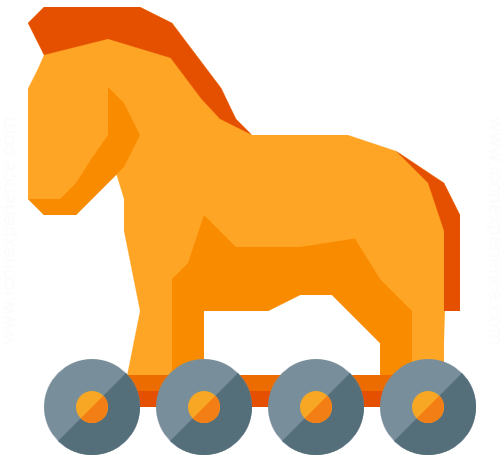
Bezpečnostní výskumníci zo spoločnosti Trustwave objavili malvér v oficiálnom čínskom daňovom softvéri Golden Tax Invoicing Software. Malvér GoldenHelper sa nachádzal v softvéri od spoločnosti Baiwang, ktorá je spolu s Aisino jediným oficiálnym dodávateľom daňového softvéru v Číne. Napriek tomu, že táto verzia softvéru je od spoločnosti Baiwang, je digitálne podpísaná dcérskou spoločnosťou Aisino. Preto je možné, že zdroj oboch malvérov je rovnaký. Kampaň na šírenie GoldenHelper pravdepodobne prebehla v rokoch 2018 a 2019, teda pred šírením GoldenSpy. Keďže kampaň skončila skôr ako výskumníci objavili malvér, škodlivý kód ktorý si malvér sťahoval zo serverov už nie je možné získať. Z tohto dôvodu nie sú známe všetky jeho schopnosti.

TLP: White

Ruská skupina APT29 sa zamerala na výskumníkov COVID-19 vakcíny

Britské National Cyber Security Centre (NCSC) vydalo správu na ktorej sa podieľali s NSA, CISA a kanadským CSE. Podľa správy počas roku 2020 skupina APT29 cielila na organizácie zapojené v tvorbe vakcíny proti COVID-19 v Kanade, Veľkej Británii a Spojených štátoch. Skupina získavala prístup do sietí organizácií cez spear-phishing a využívaním nezaplátaných zraniteľností. Vo vnútornej sieti potom stiahli svoj vlastný malvér WellMess a WellMail s cieľom vzdialene ovládať počítače a posielať výsledky na riadiaci server. Podľa NSC je APT29 takmer s určitosťou časťou ruských spravodajských služieb. Kremeľ tieto obvinenia odmieta.

Trojan Emotet sa vracia po 5 mesiacoch nečinnosti



Botnetový malvér Emotet bol v roku 2019 najviac aktívnym malvérom, ale od 7.2.2020 do 17.7.2020 zastavil všetku svoju aktivitu. Emotet sa šíri cez spamové maily a sťahuje sa v makrách súborov MS Word, ktoré sú v prílohách spamu. V aktuálnej kampani bola pridaná nová funkcionalita – Emotet kradne emailové prílohy z emailov obete, aby ich neskôr využil pri svojom šírení. V tejto kampani bolo len za jeden deň poslaných 250 000 emailov. Po nainštalovaní Emotet často sťahuje ďalší malvér. Najčastejšie sťahovaný bol v minulosti bankový trojan TrickBot, ktorý obsahuje množstvo škodlivej funkcionality. Teraz ho nahradil trojan QakBot ktorý sa šíri cez sieťové disky ako červ a je často využívaný bankovým malvérom. V niektorých krajinách (Nemecko, Holandsko) je najčastejšie sťahovaný ransomvér.

Tvorca bankovej aplikácie Dave utrpel únik dát

Útočník sa dostal do siete Dave a získal údaje o 7,5 milióna zákazníkoch. Údaje obsahovali mená, adresy, telefónne čísla, emaily, rodné čísla, šifrované Social Security čísla a hashované heslá. Dáta neobsahovali údaje o bankových účtoch a kreditných kartách. Prístup do siete bol získaný následkom skoršieho incidentu ich bývalého partnera Waydev. Waydev je analytický nástroj pre Git. Začiatkom júla útočníci kompromitovali GitHub OAuth tokeny aplikácie Waydev a získali projekty pripojených používateľov. Polícia momentálne vyšetruje tvrdenie útočníka, že prelomil niektoré heslá a predáva dáta zákazníkov Dave. Databáza bola predaná na hackerskom fóre a neskôr dostupná zadarmo na inom fóre, ale heslá neboli prelomené.

Za ransomvérom VHD stojí Severná Kórea

Výskumníci zo spoločnosti Kaspersky vydali správu podľa ktorej za takzvaným VHD ransomvérom stojí útočná skupina Lazarus zo Severnej Kórei. Pri analýze incidentov v ktorých bol použitý VHD ransomvér, výskumníci odhalili reťaz útoku, pri ktorej bol použitý malvérový framework MATA, ktorý inštaloval VHD. Kaspersky spája MATA so skupinou Lazarus kvôli unikátnym názvom súborov, ktoré táto skupina použila v minulosti v malvéri Volgmer. Kombinácia frameworku MATA a ransomvéru VHD bola použitá pri útokoch v európskych krajinách, Indii, Južnej Kórei a Japonsku.

- Platforma OneClass určená na e-learning sprístupnila údaje o študentoch a lektoroch
- Súd v Spojenom kráľovstve nariadil ukončenie činnosti platformy na obchodovanie s kryptomenami s názvom GPay
- Doteraz nepoznaná kampaň APT skupín sa zameriavala na sledovanie ujgurskej etnickej menšiny pomocou Android spywaru
- Podrobnosti o metóde obídenia ochrany súkromia v systéme macOS boli zverejnené po tom, čo Apple neposkytol opravu tejto zraniteľnosti
- Nástroj na nastavenie pozadia v systéme Windows 10 mohol byť zneužitý na stiahnutie škodlivého softvéru
- Bolo odhalených 16 aplikácií na Facebooku, ktoré tajne poskytovali údaje tretím stranám
- Podniky v Amerike a Európe boli cieľom krádeže informácií pomocou malvéru Valak
- Útočníci stojaci za ransomvérom Sodinokibi (REvil) požadujú od brazílskej energetickej spoločnosti výkupné 14 miliónov dolárov
- Nový ransomvér s názvom Try2Cry sa šíri pomocou infikovaných USB zariadení
- Skupina útočníkov známa ako Keeper je zodpovedná za porušenie bezpečnosti na viac ako 570 eshopoch za posledné tri roky
- Americké ministerstvo spravodlivosti obvinilo útočníka známeho ako "Fxmsp" za hackovanie a predaj prístupu k viac ako tristo organizáciám na celom svete
- Na hackerských fórach je momentálne v obehu viac ako 15 miliárd prihlasovacích údajov
- V Obchode Play sa v rámci 11 aplikácií opäť objavil malvér s názvom Joker
- Nová skupina ransomvéru Conti s podobným kódom ako malvér Ryuk je zameraná na podnikové siete

- **Útočník pochádzajúci z Ruska bol uznaný vinným z útoku na online platformy LinkedIn, Formspring a Dropbox**

- **Štyri sofistikované rodiny malwaru kolektívne nazvané Tetrade sa aktívne šíria do nových krajín, vrátane USA**

- **Nový trójsky kôň nazývajúci sa BlackRock napáda Android zariadenia a kradne prihlasovacie údaje a informácie o kreditných kartách zo zoznamu 337 aplikácií**

- **Služba na tvorenie videí Promo.com potvrdila únik viac ako 22 miliónov používateľských údajov**

- **Severokórejská APT skupina Lazarus využívala framework MATA pri útokoch na podnikové subjekty z viacerých krajín za účelom šírenia ransomvéru a krádeže údajov**

- **Botnet Prometei využíva zraniteľnosť vo Windows protokole SMB na ťažbu kryptomeny**

- **Phishingová kampaň využíva služby Google Cloud Services na odcudzenie prihlasovacích údajov do Office 365**

Závažné zraniteľnosti bežných softvérových produktov

Kritická zraniteľnosť v produktoch F5

Spoločnosť F5 vydala bezpečnostné aktualizácie, ktoré opravujú kritickú bezpečnostnú zraniteľnosť produktov BIG-IP s hodnotou CVSS skóre 10. Túto zraniteľnosť môže zneužiť útočník na celkovú kompromitáciu informačného systému ku ktorému má zraniteľné zariadenie prístup.

Dve kritické zraniteľnosti vo virtuálnom grafickom rozhraní produktov VMware

Spoločnosť VMware vydala bezpečnostné aktualizácie na opravu viacerých zraniteľností v programoch VMware ESXi, Workstation a Fusion. Dve najzávažnejšie z nich umožňujú vykonávať kód na hypervízorovi z virtuálneho zariadenia.

Kritické zraniteľnosti v TCP/IP knižnici pre zariadenia IoT

Bezpečnostná výskumná skupina JSOF objavila 19 zraniteľností v knižnici spoločnosti Treck protokolov TCP/IP využívanú vyše 20 rokov v IoT zariadeniach, ktoré nazvala Ripple20. 5 z 19 je klasifikovaných podľa CVSS skóre ako „High“, ostatné „Medium“ alebo „Low“. Chyby sa týkajú protokolov IPv4, IPv6, UDP, DNS, DHCP, TCP, ICMPv4 a ARP.

V systéme Palo Alto PAN-OS bola objavená kritická bezpečnostná zraniteľnosť

V protokole SAML sa nachádza kritická zraniteľnosť. Táto chyba sa nachádza v kontrolných mechanizmoch autentifikácie. Nesprávne overovanie podpisov v protokole SAML systému PAN-OS, umožňuje neoverenému útočníkovi v sieti pristupovať ku chráneným zdrojom. Aby mohol útočník zraniteľnosť zneužiť, musí získať sieťový prístup na postihnutý server.

TLP: White

Kritická zraniteľnosť v produktoch SAP

Spoločnosť Onapsis v máji objavila a ohlásila kritickú zraniteľnosť v produktoch spoločnosti SAP (CVSS 10). Spoločnosť SAP vydala záplatu na kritickú zraniteľnosť, ktorá sa nachádza v jej komponente NetWeaver. Zraniteľnosť umožňuje neautentifikovanému útočníkovi vytvárať účty s najvyššími oprávneniami a vykonávať systémové príkazy, teda úplne kompromitovať systémy využívajúce zraniteľné produkty SAP, pristupovať k citlivým údajom a zasahovať do operácií spoločnosti.

SIGRed - kritická zraniteľnosť Windows DNS serverov

Spoločnosť Microsoft opravila kritickú zraniteľnosť DNS (CVSS 10), ktorá je vo všetkých systémoch Windows Server konfigurovaných ako DNS už 17 rokov. Útočníkovi umožňuje preposielať citlivé dáta na svoj server, manipulovať so sieťovým prenosom, a tiež kompromitovať celú sieť.

Kritické zraniteľnosti v produktoch spoločnosti Adobe

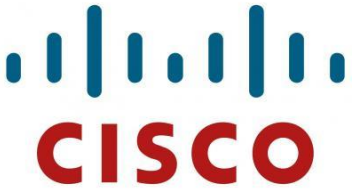
Spoločnosť Adobe vydala záplatu opravujúcu kritické zraniteľnosti vo svojich produktoch Photoshop, Bridge a Prelude. 12 kritických zraniteľností vo verziách produktov pre Windows je spôsobených možnosťou čítať a zapisovať mimo hraníc, čo môže viesť k vykonaniu ľubovoľného kódu.

Chyba vo funkcii Vanity URL aplikácie Zoom umožňuje vydávať sa za používateľa tejto funkcie

Funkcia Vanity URL v aplikácii Zoom slúžiaca na vytvorenie vlastnej URL nie je chránená proti impersonácii. K pozvánke na stretnutie je možné uviesť akúkoľvek subdomény, vďaka čomu môže vyzerať rovnako ako pozvánka od spoločnosti, ktorá túto doménu používa. Spoločnosť Zoom Video Communications vydala na túto chybu záplatu.

TLP: White

Kritické zraniteľnosti produktov Cisco



V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco AnyConnect Secure Mobility Client CVE-2020-3432: Zraniteľnosť v produkte sa nachádza v komponente na odinštalovanie a vzniká pretože aplikácia nedokáže správne spracovať cestu k adresáru. Útočník môže tento problém využiť na poškodenie obsahu ľubovoľného súboru v súborovom systéme vytvorením symbolického odkazu.
Cisco Digital Network Architecture Center CVE-2020-3391: Produkt je náchylný na chybu zverejnenia informácií, pretože ukladá poverenia v nešifrovanom formáte. Útočník môže tento problém využiť sledovaním konfigurácie sieťového zariadenia a získaním oprávnení na správu sieťových zariadení..
Multiple Cisco Unified Communications Products CVE-2020-3282: Viaceré produkty zjednotenej komunikácie sú náchylné na XSS zraniteľnosť, pretože nedokážu správne ošetriť vstupy poskytnuté používateľmi. Tento problém sa týka najmä webového rozhrania pre správu.
Cisco Unified Communications Manager CVE-2020-3420: Produkt je náchylný na HTML Injection zraniteľnosť, pretože nedokáže správne ošetriť vstupy poskytnuté používateľmi. Tento problém sa týka najmä webového rozhrania pre správu.
Cisco Unified Customer Voice Portal CVE-2020-3402: Customer Voice Portal kvôli nesprávnej autentifikácii RMI listenerov umožňuje únik citlivých informácií. Konkrétne tento problém existuje v Java Remote Method Invocation rozhraní.

Mesačník zraniteľností Júl 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
    - Kritická zraniteľnosť v produktoch F5
    - Dve kritické zraniteľnosti vo virtuálnom grafickom rozhraní produktov VMware
    - Kritické zraniteľnosti v TCP/IP knižnici pre zariadenia IoT
    - V systéme Palo Alto PAN-OS bola objavená kritická bezpečnostná zraniteľnosť
    - Kritická zraniteľnosť v produktoch SAP
    - SIGRed - kritická zraniteľnosť Windows DNS serverov
    - Kritické zraniteľnosti v produktoch spoločnosti Adobe
    - Chyba vo funkcii Vanity URL aplikácie Zoom umožňuje vydávať sa za používateľa tejto funkcie

https://www.csirt.gov.sk/aktualne-7d7.html?id=222