ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Február 2020

Vypracoval: CSIRT.SK

TLP: White

Vďaka moderným technológiám môžeme pristupovať k internetu pomocou rozličných zariadení. Avšak spolu s príchodom nových technológií sa rovnakou rýchlosťou rozvíjajú aj bezpečnostné hrozby. Preto všetky prístroje, ktoré používame sú potenciálne náchylné na zneužitie neoprávnenými používateľmi. Z tohto dôvodu je dôležité chrániť ich pomocou hesiel.

Zatiaľ čo čakáme na bezpečnejšie a pritom intuitívne riešenie autentifikácie, ktoré by si našlo cestu k bežnému používateľovi a dosiahlo širokú adaptáciu, musíme nájsť spôsob, ako minimalizovať riziká spojené s používaním hesiel. V súčasnosti však viac ako 80% útokov súvisí práve so slabými alebo ukradnutými heslami, čo ukazuje, že používatelia ešte stále nie sú dostatočne oboznámení s rizikom využívania slabých hesiel.

Rovnako veľkým problémom je taktiež využívanie rovnakého alebo príliš podobného hesla vo väčšine svojich používateľských kont. Štatistika, ktorú vypracovala spoločnosť Lastline Inc. hovorí, že 45% ľudí využíva rovnaké heslo pri väčšine registrácií. Opätovné používanie hesiel vo viacerých účtoch značne uľahčuje útočníkom kompromitovanie ďalších účtov vrátane prístupu k firemným údajom, čo im umožňuje dostať sa k dôverným alebo osobným informáciám.

K úniku údajov dochádza takmer každý deň. Väčšinou sú to emailové adresy, heslá, čísla kreditných kariet a iné citlivé údaje. Veľa ľudí žiaľ prehliada závažnosť problému, kým sa sami nestanú obeťou. Nie je však prekvapením, že miera kriminality spojená s krádežou identity podľa nedávnej štúdie stúpa. Len v Spojených štátoch sa objavuje nová obeť krádeže identity každé dve sekundy. Spoločnosť Experian zverejnila štatistiky, ktoré ukazujú, že 31% obetí, ktorých údaje boli zverejnené, boli neskôr obeťou krádeže identity. Úniky údajov sa zjavne stali súčasťou moderného života. Jedným z hlavných riešení, ako predísť problému krádeže identity, je používanie rôznych hesiel pri všetkých svojich účtoch. Akonáhle uniknú prihlasovacie údaje k určitému účtu, útočníci môžu testovať tieto údaje na širokom rozmedzí webových stránok. Ak používatelia opakovane používajú rovnaké prihlasovacie údaje, útočník môže získať prístup ku veľkému množstvu informácií na rôznych stránkach a aplikáciách.

Kvôli spomenutým dôvodom je dôležitým opatrením zmena hesla periodicky za nejaké určené časové obdobie. Global Data Risk Report, ktorý spracovala spoločnosť Verizon hovorí o tom, že až 65% spoločností má viac ako 500 zamestnancov, ktorých platnosť hesla nikdy nevyprší. Takíto používatelia poskytujú útočníkom veľké časové okno, aby tieto heslá prelomili útokom hrubou silou. Akonáhle sa im to podarí, získavajú neobmedzený prístup k údajom. Heslá, ktoré sa nemenia, majú často vyššiu pravdepodobnosť, že sa objavia práve v uniknutých zoznamoch hesiel. Správcovské účty s heslami, ktorých platnosť nikdy nevyprší sú v súčasnosti najlepším priateľom útočníka.

Aké opatrenia pre zaistenie silných a bezpečných hesiel by ste mali využívať aby ste sa nestali obeťou?

- Používajte dvojstupňovú autentifikáciu pre väčšiu bezpečnosť. Tá poskytuje ďalšiu úroveň ochrany a znemožní neoprávnený prístup k vášmu účtu. Vždy, keď budete chcieť získať

prístup k svojmu účtu, budete vyzvaní na potvrdenie svojej totožnosti aj inou formou než heslom, napríklad pomocou bezpečnostného kódu, ktorý dostanete v textovej správe.

- Vyhnite sa webom, ktoré nevyužívajú SSL certifikát. Protokol SSL/TLS šifruje údaje medzi prehliadačmi a webovými stránkami, takže informácie o bankovom účte, osobné údaje, prihlasovacie heslá a čokoľvek iné sa prenášajú šifrované. Tým pádom je menej pravdepodobné, že padnú do rúk útočníka. Preto si stále overte, že stránka používa https protokol a má platný certifikát.
- Prehodnoťte svoju stratégiu správy hesiel. Najsilnejšie heslá obsahujú 16 a viac znakov a zahŕňajú malé a veľké písmená, ako aj špeciálne znaky a čísla. Heslo by nemalo obsahovať nič, čo s vami súvisí, napríklad mená domácich zvierat, vaše narodeniny a podobne. Ako už bolo spomenuté, pre každý účet používajte rôzne heslá. Ak si ich nedokážete zapamätať, je dobré používať šifrovanú kľúčenku hesiel na vašom zariadení (napríklad KeePass). Rovnako je potrebné tieto heslá často meniť.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci február riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Okrem toho CSIRT.SK riešil wiper útok na databázu, spojený s požiadavkou o výkupné za navrátenie zmazaných dát a ich nezverejnenie. Taktiež počas parlamentných volieb 29.2.2020 bol v stave pohotovosti a monitoroval situáciu.

V rámci proaktívnej činnosti varoval CSIRT.SK svoju konštituenciu pred phishingovou kampaňou šíriacou ransomvér, zneužívajúcou identity svetových univerzít. Tiež rozposlal odporúčanie na blacklisting známych phishingových domén.

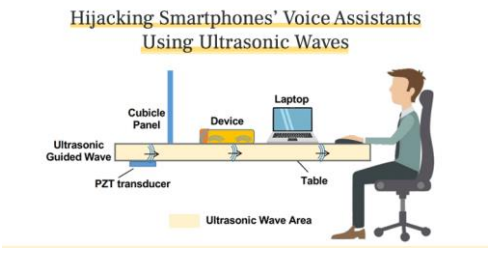
V rámci aktivít zameraných na zvyšovanie odbornej a vedomostnej úrovne tímu sa členovia CSIRT.SK zúčastnili na konferencii spoločnosti Microsoft.

Významné útoky vo svete

Unikli osobné informácie izraelských voličov

Internetová stránka volebnej kampane politickej strany Likud, ktorá je vládnucou stranou premiéra Benjamina Nethanjahua v Izraeli neúmyselne odhalila osobné informácie voličov. Pred voľbami dostávajú všetky politické strany osobné informácie o voličoch, ktoré nemôžu zdieľať so žiadnou treťou stranou. Súčasne sú zodpovedné za ochranu týchto údajov a ich vymazanie po skončení volieb. Likud údajne zdieľal celý register voličov s Feed-b, spoločnosťou zaoberajúcou sa vývojom softvéru, ktorý ho nahral na webovú stránku aplikácie Elector (elector.co.il). K incidentu došlo zverejnením administrátorského mena a hesla vo verejnom zdrojovom kóde domovskej stránky. Uniknutá databáza obsahuje celé mená, čísla občianskych preukazov, adresy a pohlavie 6 453 254 voličov v Izraeli, ako aj telefónne čísla, meno otca, meno matky a ďalšie osobné údaje niektorých z nich.

Hackeri môžu používať ultrazvukové vlny na kontrolu hlasového asistenta v zariadeniach



Vedci objavili nové prostriedky ako sa dajú kompromitovať hlasom ovládané zariadenia. Útok sa dá vykonať šírením ultrazvukových vĺn prostredníctvom pevných materiálov, aby so zariadením mohli komunikovať a kompromitovať ho pomocou nepočuteľných hlasových príkazov bez vedomia obete. „SurfingAttack“, ako sa tento útok nazýva, využíva jedinečné vlastnosti akustického prenosu v pevných objektoch ako je napríklad stôl. Útočník komunikuje so zariadeniami pomocou hlasových asistentov a tým dokáže získať dvojfaktorové autentifikačné kódy, uskutočniť podvodné hovory a podobne. Využíva vlastnosti MEMS mikrofónov, ktoré sú štandardom vo väčšine zariadení ovládaných hlasovým asistentom. Nelineárna povaha týchto mikrofónov umožňuje prenos vysokofrekvenčných zvukových vĺn, ktoré sú ľudskému uchu nepočuteľné, ale zariadenie ich dokáže dekódovať do skutočných príkazov. Aj keď dosiaľ neexistujú žiadne náznaky, že by bola táto zraniteľnosť zneužívaná, nie je to prvý krát, čo bol odhalený útok takéhoto typu.

TLP: White

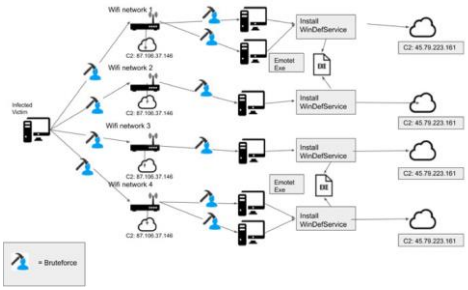
Avast Antivírus bol obvinený z predaja údajov 100 miliónov používateľov spoločnosti Google

Český Úrad na ochranu osobných údajov začal vyšetrovať firmu Avast pre predaj dát. Vyšetrovanie má zistiť, či spoločnosť Avast predávala osobné informácie zo svojej používateľskej základne spoločnostiam ako Google, Microsoft a Home Depot. Údaje, o ktorých sa predpokladá, že boli týmto spoločnostiam predané, sú história prehliadačov, vyhľadávanie na online mapách a na webe YouTube a ďalšie. Už v januári sa našli dôkazy o tom, že spoločnosť Avast zhromažďovala údaje a predávala ich prostredníctvom svojej dcérskej spoločnosti s názvom „Jumpshot“. Aj keď tieto záznamy neobsahujú IP adresu, e-mail ani iný identifikátor zákazníka, každý užívateľ má pridelené jedinečné číslo. Databáza Avastu je taká detailná, že podľa časovej osi dokáže napríklad Amazon určiť o akého klienta ide na základe porovnania časov v týchto dátach so svojou databázou. Tým pádom vie s týmito dátami ďalej pracovať, pretože okrem nákupov sledujú aj napríklad sociálne siete a históriu vyhľadávania.

Štyria čínski hackeri boli obvinení z útoku na spoločnosť Equifax

Americké ministerstvo spravodlivosti oznámilo obvinenia voči 4 čínskym vojenským hackerom, ktorí údajne stáli za únikom dát spoločnosti Equifax a odhalili osobné a finančné údaje takmer 150 miliónov Američanov. Útočníci boli tiež obvinení z krádeže obchodných tajomstiev, duševného vlastníctva a dôverných informácií od viacerých amerických podnikov. Spoločnosť Equifax oznámila, že bola obeťou tohto kybernetického útoku v roku 2017. Ich servery boli napadnuté pomocou kritickej zraniteľnosti v Apache Struts Web Framework, ktorú v tom čase nemali ošetrenú. Získali prihlasovacie údaje takmer polovice amerických občanov, vďaka ktorým získali ďalšie dáta ako ich mená, dátumy narodenia a čísla sociálneho zabezpečenia.

Emotet malvér sa začína šíriť cez Wi-Fi siete



Emotet je v súčasnosti jedným z najrozšírenejších druhov malvéru. V minulosti sa šíril infikovanými súbormi Office prenášanými pomocou emailu. Akonáhle sa zariadenie infikovalo, tento trójsky kôň sa začal šíriť na zariadenia v lokálnej sieti. Avšak spoločnosť Binary Defense identifikovala nový modul, ktorý využíva rozhranie wlanAPI na zistenie všetkých Wi-Fi sietí v tejto oblasti. Dokáže si extrahovať SSID, silu signálu, metódu autentifikácie a režim šifrovania používaný na zabezpečenie hesiel. Následne sa pokúsi pripojiť k týmto sieťam vykonaním útoku hrubou silou na heslo. Ak sa mu to podarí, vykoná druhé kolo útoku hrubou silou, aby infikoval zariadenia v danej Wi-Fi sieti. V ďalšej fáze inštaluje škodlivý softvér „service.exe“ a zariadenie začne komunikovať s riadiacim serverom, ktorý mu posiela príkazy. Binary Defense tvrdí, že modul na šírenie malvéru cez Wi-Fi vznikol v roku 2018, avšak nebol tak rozšírený, preto sa ho podarilo odchytiť až teraz.

Ransomware útok ochromil oblasť Redcar a Cleveland v Anglicku

Servery miestnych orgánov v severovýchodnej časti Anglicka utrpeli veľký ransomware útok. Webová stránka miestnej rady oblasti Redcar a Cleveland, ktorá slúžila viac ako 135 tisícom obyvateľov bola pozastavená na viac ako tri týždne. V dôsledku útoku sa občania nemohli dostať ku online rezerváciám, digitálnym dokumentm, poradenským službám sociálnej starostlivosti a systému na sťažnosti na bývanie v mestách tejto oblasti. Zo začiatku orgány tvrdili že majú iba problém s IT systémom, neskôr však priznali, že išlo o ransomvér útok. Avšak podľa všetkého zo serverov neboli odstránené žiadne osobné informácie. Na ostránení problému spolupracujú s National Cyber Security Centre (NCSC) a s National Crime Agency (NCA).

Clearview AI: Počítačová databáza zhromažďujúca tváre bola napadnutá

Spoločnosť, ktorá sa venuje rozpoznávaniu tvárí a ktorá uzatvára zmluvy s výkonnými orgánmi činnými v trestnom konaní, oznámila, že útočník ukradol celý zoznam ich klientov. Medzi nimi sa nachádza aj americký imigračný úrad (US Immigration and Customs Enforcement). Útočník získal prístup k zoznamu zákazníkov, k počtu prihlásení, dátumu posledného vyhľadávania a počtu vyhľadávaní, ktoré títo zákazníci previedli. V oznámení sa uvádza, že servery spoločnosti neboli porušené a teda „nedošlo k ohrozeniu systémov alebo siete spoločnosti Clearview“. Spoločnosť tiež uviedla, že opravila danú zraniteľnosť a že útočník nezískal históriu vyhľadávania žiadnych orgánov činných v trestnom konaní.

Spoločnosti Decathlon uniklo 123 miliónov záznamov

Francúzsky gigant na predaj športového sortimentu Decathlon bol terčom útoku pri ktorom unikli osobné informácie. Prostredníctvom nesprávne zabezpečeného servera ElacsticSearch uniklo cez 123 miliónov záznamov. Medzi dátami boli nešifrované maily a heslá zákazníkov, API logy, komplexné súkromné záznamy zamestnancov vrátane podrobností o zmluve, dátum narodenia a ďalšie. Výskumníci v spoločnosti VPNmentor si uniknutú databázu všimli 12. februára a spoločnosť Decathlon upovedomili o 4 dni neskôr. Tá zareagovala rýchlo a na zraniteľný server okamžite znemožnila prístup verejnosti.

ISS World hack zanechal tisíce zamestnancov offline

Kybernetický útok zasiahol spoločnosť ISS World, ktorá má po celom svete pol milióna zamestnancov. ISS poskytuje upratovacie, stravovacie, bezpečnostné a iné služby najmä vo Veľkej Británii. Ich webové stránky boli od 17. februára vypnuté, podľa všetkého išlo o ransomvér. ISS uviedla, že zakázala prístup k svojim IT službám a produktom ako preventívne opatrenie, keď zaznamenala útok. Spoločnosť tvrdí, že mnoho z jej 500 000 globálnych zamestnancov nevyužíva počítače pri svojej každodennej práci, avšak dopad na túto spoločnosť je veľký.

TLP: White

Nový malvér „Haken“ bol nájdený v 8 aplikáciách na Google Play Store

Nový druh škodlivého softvéru, ktorý kradne dáta a bez vedomia užívateľov ich prihlási na platený odber prémiových služieb bol objavený v ôsmich aplikáciách určených pre operačný systém Android. Tieto aplikácie, ktoré boli infikované rodinou malvéru s názvom Haken boli určené najmä ako pomôcky pre fotoaparáty a detské hry. Tento druh malvéru sa nazýva aj „klikací“, keďže napodobňuje správanie používateľa a kliká na čokoľvek, čo sa objaví na obrazovke. Tým dokáže prihlásiť stiahnuté aplikácie na odber platených služieb a takisto môže pristupovať k citlivým informáciám viditeľným na mobilnej obrazovke. Súhrnne boli dané aplikácie stiahnuté viac ako 50 000-krát a po ohlásení hrozby spoločnosti Google boli vymazané.

Masívna phishingová kampaň šíri ransomware

V súčasnosti prebieha masívna phishingová kampaň šíriaca ransomvér, ktorá zneužíva mená univerzít. Útočníci predstierajú identitu vysoko postavených zamestnancov vybranej univerzity a žiadajú od obetí, aby otvorili škodlivú prílohu pod zámienkou kontroly rozpočtu na rok 2020.

- **Dánsky daňový portál omylom zverejnil identifikačné čísla 1,26 milióna dánskych občanov.**
- **Austrálskym bankám sa vyhrážajú útočníci DDoS útokmi ak odmietnu zaplatiť.**
- **Ransomvér útok na políciu zapríčinil prepustenie 6 osôb podozrivých z predaja drog.**
- **Malvér Racoon sa zameriava na rozsiahlu škálu prehliadačov, jeho cieľom je ukradnúť dáta a kryptomeny.**
- **Cerberus Android malvér dokáže obísť 2FA a vzdialene odomknúť zariadenia.**

TLP: White

- **Americká agentúra zodpovedná za bezpečnú komunikáciu pre Biely dom sa stala obeťou kybernetického útoku a odhalila osobné údaje asi 200 000 ľudí.**

- **Boli odhalené osobné údaje 10,6 milióna hostí, ktorí boli ubytovaní v hoteloch MGM Resorts.**

- **Vo svete IoT sa rozširuje malvér Lemon Duck zameraný na operačné systémy Windows 7.**

- **250 Android aplikácií bolo cieľom phishingovej kampane, rozširujúcej malvér Anubis ktorý dokáže získať prihlasovacie údaje, dáta zo zariadenia ale aj nainštalovať keylogger.**

- **Facebook žaluje výrobcu SDK za utajené získavanie užívateľských údajov.**

- **Počítačový útok eliminoval 25% iránskeho internetu.**

- **Používateľom PayPal boli naúčtované podvodné poplatky prostredníctvom služby Google Pay.**

- **Vláda Portorika prišla kvôli phishingu o viac ako 2,6 milióna dolárov.**

- **Chyba webovej stránky spoločnosti Samsung odhalila údaje o zákazníkoch vo Veľkej Británii.**

- **Spyware aplikácia KidsGuard bola tajne nainštalovaná na tisícky telefónov, chybne nakonfigurovaný server však spôsobil, že aplikácia sprístupňovala tajne nahraný obsah zariadení obetí na internet.**

- **Nový phishingový útok sa zameriava na vlády, jeho cieľom je získať prihlasovacie údaje pomocou malvéru ForeLord.**

- **Ransomware RobbinHood používa zastaraný Windows Gigabyte driver na odstránenie antivírusových produktov.**

- **Vedci spoločnosti Checkmarx podrobne popisujú bezpečnostné problémy objavené v robotických vysávačoch. Tieto chyby by mohli hackerom poskytnúť prístup k napájaniu kamery.**

- **Americký obchodný reťazec Rutter odhalil narušenie bezpečnosti, 71 jeho prevádzok bolo infikovaných point-of-sale (PoS) malvérom, ktorý slúži na krádež informácií o kreditných kartách zákazníkov.**

Závažné zraniteľnosti bežných softvérových produktov

CDPwn - kritické zraniteľnosti Cisco protokolu CDP

Desiatky miliónov zariadení Cisco po celom svete obsahujú kritické zraniteľnosti umožňujúce vzdialené vykonávanie kódu a vyvolanie nedostupnosti služby. Tento súbor piatich zraniteľností bol nazvaný CDPwn, podľa protokolu, v ktorého implementáciách sa nachádzajú. Útočníci môžu okrem iného sledovať komunikáciu, odpočúvať telefóny, exfiltrovať dáta a úplne ovládnuť sieť, nakoľko zraniteľnosti dovoľujú prechádzať do jej iných segmentov.

Bola opravená kritická XSS zraniteľnosť vo WordPress doplnku GDPR Cookie Consent

Spoločnosť WordPress opravila kritickú zraniteľnosť, zatiaľ bez CVE čísla, vo Wordpress doplnku GDPR Cookie Consent umožňujúcu útočníkovi pozmeniť obsah alebo vložiť škodlivý cross-site scripting (XSS) obsah na webovú stránku obete. Odporúčame aktualizovať doplnok aspoň na verziu 1.8.3.

Kritická chyba vo WordPress doplnku od spoločnosti ThemeGrills

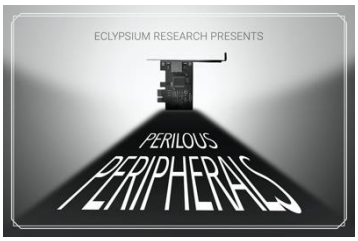
Kritická zraniteľnosť nachádzajúca sa vo WordPress doplnku ThemeGrill Demo Importer umožňuje útočníkom kompletné vymazanie obsahu celej webovej stránky a automatické prihlásenie do administrátorskému účtu na stránke, ak vymazaná databáza obsahovala účet s názvom “admin“. Odporúčame aktualizovať doplnok aspoň na verziu 1.6.2.

Spoločnosť Microsoft má problém s krádežami jej subdomén

Subdomény spoločnosti Microsoft sú často zneužívané útočníkmi pri útokoch na používateľov a zamestnancov spoločnosti a pre zobrazovanie spamových reklám, napríklad na online kasína. Ukradnuté subdomény môžu útočníci zneužiť pre zvýšenie dôveryhodnosti phishingových kampaní zameraných napríklad na získavanie prihlasovacích údajov do účtov Microsoft.

TLP: White

Milióny počítačov od Dell, HP, Lenovo a možno aj ďalších výrobcov sú zraniteľné voči firmvérovým útokom



Nedostatočné overovanie autenticity firmvérov periférnych zariadení obvykle od dodávateľov tretích strán robí milióny počítačov využívajúcich Windows alebo Linux zraniteľných voči útokom zameraným na infikovanie firmvérov škodlivým kódom. Navyše v niektorých prípadoch nepomôže ani samotná aktualizácia firmvéru.

Závažná zero-day zraniteľnosť nájdená v Google Chrome

Internetový prehliadač Google Chrome má závažnú zraniteľnosť, ktorá je aktívne zneužívaná (zero-day). Chyba spočíva v nedostatočnom overení typu premennej pred jej spracovaním (type confusion). Útočníkom umožňuje vzdialene vykonávať kód.

Chyba Ghostcat ovplyvňuje všetky verzie Apache Tomcat vydané za posledných 13 rokov

Servery Apache Tomcat vydané za posledných 13 rokov sú zraniteľné voči chybe s názvom Ghostcat, ktorá môže hackerom umožniť prevziať kontrolu nad systémom. Zraniteľnosť, ktorú objavila spoločnosť Chaitin Tech, využíva chybu v protokole AJP Tomcat. AJP znamená Apache JServ Protocol a je to verzia HTTP protokolu optimalizovaná na výkon v binárnom formáte. Tomcat používa AJP na výmenu údajov s Apache HTTPD servermi alebo inými inštanciami Tomcat. Konektor AJP Tomcat je predvolene povolený na všetkých serveroch Tomcat a počúva na serverovom porte 8009. Nájdenú zraniteľnosť je možné využiť na čítanie alebo zápis súborov na server Tomcat. Útočníci by mohli čítať konfiguračné súbory aplikácií a ukradnúť heslá alebo API tokeny. Zraniteľnosť Ghostcatu je rozsiahla, keďže ovplyvňuje všetky vetvy Tomcat 6.x, 7.x, 8.xa 9.x.

Malvér pre Android môže ukradnúť Google Authenticator 2FA kódy.

Bola objavená nová verzia trójskeho koňa s názvom "Cerberus", ktorý dokáže ukradnúť jednorazové kódy vygenerované aplikáciou Google Authenticator a obísť účty chránené dvojfaktorovou autentifikáciou. Aplikácia Authenticator funguje tak, že vygeneruje šesť až osem-miestne jedinečné kódy, ktoré používatelia musia zadať do prihlasovacích formulárov na prístup k online účtom. Využíva sa ako alternatíva k jednorazovým prístupovým kódom posielaným SMS správami. Keď je táto aplikácia spustená, trójsky kôň môže získať obsah rozhrania a odošle ho na riadiaci server.

Spoločnosť Adobe opravila 35 kritických zraniteľností v novej bezpečnostnej aktualizácii.

Väčšina opráv bola vydaná na program Adobe Framemaker. Tento program vo verzii 2019.0.4 a nižšej na operačnom systéme Microsoft Windows obsahoval celkom 21 zraniteľností, z ktorých všetky boli považované za kritické. Taktiež boli opravené zraniteľnosti ako chyby vyrovnávacej pamäte, prístup k pamäti v oblasti mimo dosahu, problémy s pretečením haldy a problémy s poškodením pamäte, pričom všetky z nich mohli viesť k vykonaniu ľubovoľného kódu. Kritické, dôležité a stredne závažné bezpečnostné nedostatky boli odstránené aj v aplikáciách Adobe Acrobat DC, Reader DC, Acrobat / Reader 2017 a Acrobat / Reader 2015 v systémoch Windows a MacOS. Avšak dve zraniteľnosti neboli opravené. Prvá, CVE-2020-3759, je dôležitou bezpečnostnou chybou vyrovnávacej pamäte, ktorú je možné využiť na únik informácií. Druhou a závažnejšou z týchto dvoch zraniteľností, CVE-2020-3760, je „command injection“ problém, ktorý je možné zneužiť na vykonanie ľubovoľného kódu.

Zyxel 0day ovplyvňuje aj ich firewall produkty

Výrobca sieťového hardvéru Zyxel vydal bezpečnostné aktualizácie, čím opravil kritickú bezpečnostnú zraniteľnosť v NAS (network attached storage), ktorú aktívne zneužívali útočníci na šírenie ransomware. Avšak táto zraniteľnosť je prítomná aj v mnohých firewall produktoch tejto spoločnosti. V aktualizovanom bezpečnostnom odporúčaní sa uvádza, že zraniteľné sú UTM, ATP a VPN firewally, na ktorých je spustená verzia firmvéru ZLD V4.35 Patch 2. Verzie firmvéru pred verziou ZLD V4.35 Patch 0 zraniteľné nie sú.

TLP: White

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:

Cisco IP Phone (CVE-2020-3111): Úspešné zneužitie tejto zraniteľnosti umožňuje útočníkovi vzdialene spustiť ľubovoľný kód s oprávneniami typu root alebo znova načítať zariadenie, čo spôsobí odmietnutie služby.

Cisco Identity Services Engine (CVE-2020-3149): Zneužitie môže mať za následok vykonanie HTML a skriptovacieho kódu útočníkom v kontexte zraniteľnej aplikácie, čo mu potenciálne umožní ukradnúť prihlasovacie údaje založené na súboroch cookie alebo ovládať spôsob vykresľovania stránky používateľovi.

Cisco Cloud Web Security (CVE-2020-3154): Aplikácia je náchylná na zraniteľnosť pomocou SQL injekcie, pretože nedokáže dostatočne ošetriť vstup zadaný používateľom pred použitím v SQL dopyte.

Cisco Data Center Network Manager (CVE-2020-3113): Zneužitie zraniteľnosti je rovnaké ako u CVE-2020-3149 uvedenej vyššie.

Cisco Email Security Appliance (CVE-2019-1947): Aplikácia je náchylná na útok zahltením servera služby (DoS), pretože nedokáže správne spracovať e-mailové správy, ktoré obsahujú veľké prílohy. Úspešné zneužitie umožňuje útočníkovi spôsobiť trvalý stav DoS kvôli vysokému využitiu CPU.

Cisco Identity Services Engine (CVE-2020-3156): Zneužitie zraniteľnosti môže útočníkovi umožniť vykonanie ľubovoľného kódu v kontexte zraniteľného rozhrania alebo prístup k citlivým informáciám založeným z prehliadača.

Cisco Smart Software Manager On-Prem Default Credentials (CVE-2020-3158): Aplikácia je náchylná na chybu zabezpečenia neoprávneného prístupu. Zraniteľnosť sa týka systémových účtov, ktoré majú prednastavené a statické heslo a nie sú pod kontrolou systémového administrátora. Úspešné zneužitie povoľuje útočníkovi obdržať práva čítať a zapisovať do systémových súborov a ku konfigurácii zraniteľného zariadenia.

Cisco Unified Contact Center Express (CVE-2019-1888): Vzdialený útočník môže zraniteľnosť zneužiť na získanie zvýšených oprávnení na zraniteľných zariadeniach.

Cisco FXOS Software (CVE-2020-3166): Zraniteľnosť sa týka nesprávneho ošetrenia vstupu v príkazovom riadku, jej zneužitie môže útočníkovi umožniť čítať a zapisovať ľubovoľné súbory do základného operačného systému.

Cisco NX-OS Software (CVE-2020-3174, CVE-2020-3175): Zraniteľnosť CVE-2020-3174 sa týka zabezpečenia vzdialeného prístupu a útočníkovi môže umožniť obídenie bezpečnostných obmedzení a vykonanie neoprávnených akcií. Zraniteľnosť CVE-2020-3175 súvisí s nesprávnou kontrolou využívania zdrojov a jej zneužitie môže vytvoriť podmienky na útok zahltením servera služby (DoS).

Zraniteľnosti VMware

V produktoch VMware bolo opravených viacero rozličných kritických a závažných zraniteľností:
CVE-2020-3943: Zraniteľnosť sa týka vykonávania vzdialeného kódu a jej zneužitie môže vytvoriť podmienky na útok zahltením servera služby (DoS).
CVE-2020-3944: Zraniteľnosť sa týka zabezpečenia overenia používateľa a jej zneužitie môže útočníkovi umožniť vykonanie neoprávnených akcií.
CVE-2020-3945: Zraniteľnosť sa týka zverejnenia informácií a jej zneužitie môže neoprávnenému používateľovi umožniť získanie citlivých informácií.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero rozličných kritických a závažných zraniteľností:
Intel Converged Security Management Engine (CVE-2019-14598): Zraniteľnosť sa týka zabezpečenia overenia lokálneho používateľa a jej zneužitie môže vytvoriť podmienky na útok zahltením servera služby (DoS) alebo na získanie citlivých informácií.
Intel RAID Web Console 3 (CVE-2020-0564): Aplikácia je je náchylná na zraniteľnosť spôsobenú lokálnou eskaláciou oprávnení, zneužitie zraniteľnosti umožňuje útočníkovi získať zvýšené privilégiá.
Intel Renesas Electronics USB 3.0 Driver (CVE-2020-0560): Zraniteľnosť umožňuje útočníkovi získať zvýšené privilégiá.
Intel predstavil zhrnutie svojich bezpečnostných aktivít na konferencii RSA 2020 v San Franciscu. Spoločnosť uviedla, že v roku 2019 opravili 256 bezpečnostných nedostatkov, z ktorých 11 prípadov bol zraniteľný práve procesor. Medzi nahlásené problémy patrili napríklad Zombieload, RIDL, Fallout, SWAPGSAttack, Zombieload v2 a NetCAT. Všetky uvedené chyby úzko súviseli so závažnými zraniteľnosťami Meltdown a Spectre, ktoré boli tiež objavené ešte v roku 2018.

Mesačník zraniteľností Február 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
    - CDPwn
    - XSS zraniteľnosť vo WordPress doplnku GDPR Cookie Consent
    - Kritická chyba vo WordPress ThemeGrills Demo Importer
    - Dell, HP, Lenovo zraniteľné voči firmvérovým útokom
    - Kritická zraniteľnosť Cisco Smart Software Manager On-Prem

https://www.csirt.gov.sk/aktualne-7d7.html?id=208