MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK
Máj 2020

Vypracoval: CSIRT.SK

TLP: White

V dnešnej dobe sa stáva samozrejmosťou, že každý deň dochádza k únikom citlivých údajov z rôznych zdrojov. Najčastejšou príčinou takýchto únikov je malvér. Anglické slovo „malware“ vzniklo spojením slov „malicious“ a „software“, označuje teda škodlivý kód. V priebehu tohto roka je čoraz častejšie pozorovaný malvér využívajúci vzdialený prístup, teda po infikovaní týmto malvérom má útočník prístup k napadnutému zariadeniu.

Jedným z rozšírených typov malvéru využívajúcich vzdialený prístup je takzvaný Remote Access Trojan (RAT), ktorý predstavuje trójskeho koňa so vzdialeným prístupom. Trójsky kôň je malvér, ktorý maskovaním skrýva svoju škodlivú aktivitu. Ak trójsky kôň umožňuje vzdialený dohľad, či prístup do infikovaného zariadenia, nazývame ho RAT. Takéto malvéry často napodobňujú chovanie keyloggerov tým, že umožňujú automatizovaný zber stlačení klávesov, používateľských mien, hesiel, snímok obrazovky, histórie prehliadača, e-mailov, chatov atď. Rozdiel medzi RAT a keyloggerom je v tom, že RAT poskytuje útočníkovi možnosť získať neautorizovaný vzdialený prístup k počítaču obete pomocou špeciálne nakonfigurovaných komunikačných protokolov. Tie sú nastavené pri počiatočnej infekcii počítača obete.

V poslednom polroku azda najrozšírenejší z tohto typu malvéru je Agent Tesla RAT. Tento malvér bol zaznamenaný už v roku 2014 a hoci sa považuje za trójskeho koňa, jeho autori tvrdia niečo iné. Agent Tesla bol na svojej oficiálnej stránke (ktorá však už neexistuje) predávaný s licenciou ako sledovací softvér, určený pre počítače ku ktorým autori stiahnutého produktu majú plný prístup. Jeho cieľom teda bolo zabezpečenie vlastného softvéru pred útočníkmi a slúžiť mal ako nástroj vzdialenej správy.

Netrvalo však dlho a nástroj Agent Tesla bol označený ako škodlivý softvér. Tento malvér je schopný získavať informácie z rôznych prehliadačov, ale aj emailových a FTP klientov. Okrem toho zbiera uložené heslá, kopíruje dáta, zachytáva snímky obrazovky a zbiera dáta z vypĺňaných formulárov. Navyše jeho autor na svojej stránke vysvetľoval ako je možné tento malvér nainštalovať na počítač bez toho, aby o tom vedel jeho majiteľ. Agent Tesla sa zvyčajne dostane do infikovaného počítača pomocou súboru, na ktorý obeť klikne a tým si malvér stiahne.

Ďalším príkladom RAT malvéru, ktorého aktivita bola rozšírená aj v poslednom polroku je NetWire RAT. Rovnako ako Agent Tesla sa NetWire šíri pomocou súborov, ktoré sú najčastejšie prílohou phishingovej emailovej správy. NetWire teda môže byť ukrytý v obrázku, v PDF súbore či v súbore programu Microsoft Word. Pomocou vložených makier a PowerShell kódu malvér následne zbiera dostupné údaje z kompromitovaného počítača.

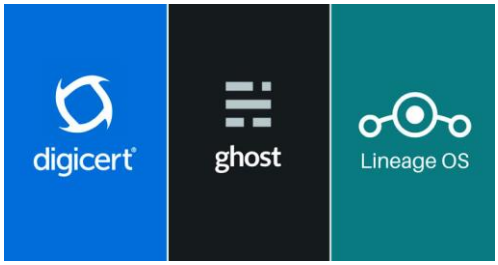
Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci máj riešil najmä phishingové kampane na svoju konštituenciu. Okrem toho CSIRT.SK vykonal forenznú analýzu PC s podozrením na kompromitáciu, ktorý patril organizácii v jeho konštituencii a tiež incident spojený s podozrením na únik dát.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK informovala svoju konštituenciu o aktívnom zneužívaní zraniteľností produktov Sophos a Draytek. Taktiež informovala o niekoľkých kampaniach šíriacich malvér Emotet a Trickbot, pričom rozposlala indikátory kompromitácie (IP adresy) pre blacklisting. Rozposlané bolo aj varovanie pred kampaňou APT skupiny Berserk Bear, spolu s indikátormi kompromitácie (IP a URL adresy, haše) pre blacklisting a kontrolu kompromitácie. CSIRT.SK sledoval dianie okolo skupiny APT38 Lazarus, ktorá bola aktívna aj na Slovensku.

Významné útoky vo svete

Zraniteľnosti v softvéri Salt umožnili napadnutie serverov LineageOS, Ghost a DigiCert



Bezpečnostní analytici spoločnosti F-Secure v máji odhalili 2 zraniteľnosti v softvéri Salt spoločnosti SaltStack. Keďže tie neboli spoločnosťou opravené ihneď po vydaní reportu, útočníci ich stihli niekoľko dní po ich vydaní využiť vo svoj prospech. V niektorých prípadoch napadnutí útočníci nasadili zadné vrátka na napadnuté servery. Neopravené zraniteľnosti umožnili kompromitáciu serverov LineageOS, Ghost a DigiCert na niekoľko dní.

Logistickú spoločnosť Toll Group zasiahol ransomvér už druhýkrát za tri mesiace

Po prvýkrát bola spoločnosť Toll napadnutá vo februári ransomvérom s názvom Netwalker. V máji čelia ďalšiemu útoku. Spoločnosť pozastavila niektoré svoje IT systémy po detegovaní nezvyčajnej aktivity na svojich serverov. Vyšetrovanie odhalilo, že sa jednalo o infekciu ransomvérom Nefilim, ktorý bol objavený len nedávno. Najčastejšie sa šíri pomocou RDP protokolu. Je si podobný s inými rodinami ransomvérov, ako napríklad Nemty, Crysis a SamSam. Autori potvrdili, že tento škodlivý softvér je určený na krádež údajov. V polovici mája ich začali zverejňovať, pretože im nebolo vyplatené výkupné.

Vláda USA našla 3 nové druhy malvéru používané severokórejskou hackerskou skupinou

Vláda USA zverejnila informácie o troch nových kmeňoch škodlivého softvéru pochádzajúceho zo Severnej Kórei. Tie sa nazývajú COPPERHEDGE, TAINTEDSCRIBE a PEBBLEDASH. Sú schopné spoločného prieskumu a exfiltrácie citlivých informácií z cieľových systémov. COPPERHEDGE je nástroj pre vzdialený prístup (RAT), ktorý je schopný spúšťať ľubovoľné príkazy, vykonávať prieskum systému a exfiltráciu. TAINTEDSCRIBE funguje ako zadné dvierka, ktorý umožňuje sťahovať škodlivý kód z riadiaceho servera a vykonávať ho. Posledný, PEBBLEDASH je trójsky kôň, ktorý môže sťahovať, posielať, mazať a spúšťať súbory.

TLP: White

Skupina útočníkov predáva milióny používateľských záznamov na dark webe

Hackerská skupina známa pod menom Shiny Hunters zaplavila dark web databázami obsahujúcimi 73,2 milióna záznamov o používateľoch z 11 rôznych spoločností. Medzi ne patria Zoosk, Chatbooks, SocialShare, Home Chef, Minted, Chronicle of Higher Education, GGuMim, Mindful, Bhinneka a Startribune. Rovnaká skupina stála za únikom dát spoločnosti Tokopedia, ktorá prevádzkuje najväčší internetový obchod v Indonézii. Uniknutá databáza obsahovala 90 miliónov záznamov a predávala sa za 5000 dolárov. Spoločnosť BleepingComputer potvrdila, že predávané záznamy sú legitímne a oboznámila napadnuté spoločnosti o tomto incidente.

Zo súkromných repozitárov GitHubu boli ukradnuté dáta

Útočník získal prístup k účtu GitHub zamestnanca spoločnosti Microsoft a získal prístup k niektorým z privátnych repozitárov. Predpokladá sa, že útočník získal cez 500GB dát. K tomuto útoku sa priznala skupina Shiny Hunters, ktorá stojí za viacerými únikmi dát v tomto mesiaci. Na hackerskom fóre bola zverejnená časť z týchto dát o veľkosti 1GB. Na základe časových pečiatok súborov bolo zistené, že k úniku došlo už 28. marca. K týmto dátam nepatrili žiadne interné projekty spoločnosti Microsoft. Podľa ich slov ich majú uložené na súkromných serveroch.

Texaské súdy boli zasiahnuté ransomvérom

Úrad pre súdnu správu (OCA), ktorý poskytuje IT služby štátnym justičným agentúram potvrdil, že ich súdny systém v štáte Texas bol napadnutý ransomvérom. Úrad však trvá na tom, aby nevyplatil žiadne výkupné. Tesne po útoku boli prepojené severy a webové stránky vypnuté, aby sa predišlo ďalšej kompromitácii. Podľa autorít neexistujú žiadne indikátory toho, že by boli kompromitované citlivé alebo osobné údaje.

Priemyselné firmy boli zasiahnuté malvérom distribuovaným skupinou RATicate

Výskumníci v oblasti bezpečnosti zo spoločnosti Sophos identifikovali skupinu útočníkov, ktorí zneužívali NSIS inštalátory na nasadenie nástrojov na vzdialený prístup (RAT) a malvér určený na krádež informácií. Tieto útoky sa zameriavajú na priemyselné spoločnosti z Európy, Blízkeho východu a Kórei. Medzi ne patria výrobcovia elektrických zariadení, internetové spoločnosti, stavebná a inžinierska spoločnosť a podobne. Táto RAT infekcia umožňuje zariadeniu zadávať príkazy na vykonávanie škodlivej aktivity, ako napríklad zaznamenávanie stlačených kláves, posielanie spamu, aktivácia webovej kamery na diaľku a podobne.

Ransomvér šifruje z virtuálnych strojov, aby sa vyhol antivírusu

Nový ransomvér s názvom Ragnar Locker sa zameriava na korporátne siete pri útokoch na spoločnosti. Tento druh škodlivého kódu nainštaluje na zariadenie aplikáciu VirtualBox a spustí virtuálny stroj s operačným systémom Windows XP. V ňom následne spustí ransomvér s cieľom vyhnutia sa antivírusovému programu. Odtiaľ šifruje súbory na hostiteľskom systéme. Z hľadiska antivírusového softvéru sú súbory len nahradené ich šifrovanými verziami a všetky zmeny prichádzajú z legitímneho procesu – aplikácie VirtualBox. Po ukončení šifrovania nájde obeť súbor so správou ktorá hovorí, že spoločnosť bola napadnutá a súbory zašifrované.

Útočníci kompromitovali servery spoločnosti Cisco pomocou zraniteľnosti SaltStack

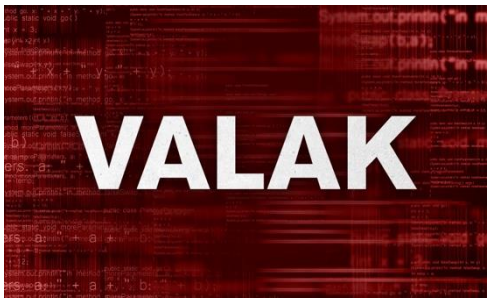
Spoločnosť Cisco uviedla, že útočníci využili zraniteľnosť v softvérovom balíku SaltStack na získanie prístupu k šiestim serverom. Tie poskytujú backend infraštruktúru pre VIRL-PE (Internet Routing Lab Personal Edition), čo je služba umožňujúca vytvárať architektúry virtuálnych sietí na testovanie pred reálnym nasadením. Bolo zistené, že boli napadnuté servery Cisco, ktoré obsahujú služby Cisco VIRL-PE verzie 1.2 a 1.3. Táto zraniteľnosť ovplyvnila aj nástroj Cisco Modeling Labs Corporate Edition. Záplaty na tieto zraniteľnosti boli vydané koncom mája.

TLP: White

Europol zatkol útočníkov z hackerskej skupiny Infinity Black

Poľské a švajčiarske orgány činné v trestnom konaní zatkli s podporou Europolu päť osôb v Poľsku, o ktorých sa predpokladá, že sú súčasťou skupiny Infinity Black. Súčasne boli zadržané elektronické zariadenia, externé disky a hardvérové peňaženky kryptomien v hodnote približne 108 tisíc dolárov. Polícia tiež ukončila prevádzku dvoch platforiem, na ktorých sa nachádzali databázy s viac ako 107 miliónmi záznamov. Útočníci prevádzkovali kanály Discord a súčasne aj viacero vlákien na hackerských fórach. Útočníci vytvorili nástroj, vďaka ktorému získali prístup k švajčiarskym používateľským účtom, čo vyústilo k predpokladanej strate 50 tisíc eur.

Malvér Valak sa zameral na servery Microsoft Exchange s cieľom kradnúť podnikové údaje



V posledných 6 mesiacoch malvér Valak zmenil svoju aktivitu na kradnutie informácií zo zariadenia. Na podniky v USA a v Nemecku bola použitá phishingová kampaň s cieľom získať informácie z emailov, heslá a certifikáty. Tento malvér sa zameriava na servery Microsoft Exchange. Výskumníci zo spoločnosti Cybereason Nocturnus zistili, že Valak umožňuje útočníkom vykonávať prieskum a kradnúť informácie pomocou vložených komponentov. Dokáže ukryť svoju aktivitu a využíva únikové techniky, ako napríklad alternatívne dátové toky (ADS).

Spoločnosť EasyJet potvrdila kybernetický útok na 9 miliónov ich klientov

EasyJet, najväčšia letecká spoločnosť v Spojenom kráľovstve, oznámila, že dôsledkom útoku boli odhalené e-mailové adresy a cestovné informácie 9 miliónov zákazníkov. U niektorých týchto zákazníkov mali útočníci prístup k podrobnostiam o kreditných kartách. Tento útok bol spoločnosťou EasyJet oznámený britskému národnému stredisku pre kybernetickú bezpečnosť a ICO. Spoločnosť uvádza, že upozornila dotknutých zákazníkov. Letecká spoločnosť nezverejnila presne, ako k prieniku došlo, kedy k nemu došlo, kedy ho spoločnosť objavila ani ako dlho mali útočníci prístup do systémov leteckej spoločnosti.

- **Akademici ukázali, ako sa dá zmeniť zdroj napájania na reproduktor, ktorý dokáže tajne prenášať údaje pomocou zvukových vĺn**
- **Útočníci, o ktorých sa predpokladá, že pôsobia v záujme čínskej vlády, sa zamerali na fyzicky izolované vojenské siete na Taiwane a Filipínach**
- **Analytici našli nové vzorky malvéru Ramsay, ktorý dokáže zhromažďovať citlivé súbory zo systémov izolovaných od internetu**
- **Nový botnet s názvom Kaiji napáda IoT zariadenia a počítače s operačným systémom Linux pomocou útoku hrubou silou na službu SSH**
- **Útočníci sa zamerali na viac ako 900 tisíc webových stránok WordPress prostredníctvom zraniteľností v ich doplnkoch a motívoch**
- **Spoločnosť GoDaddy varovala zákazníkov, že útočníci mohli získať prihlasovacie údaje do webhostingu**
- **Vyhľadávacia služba Algolia uviedla, že došlo k získaniu neoprávneného prístupu k ich infraštruktúre využitím zraniteľnosti na serveroch Salt**
- **Dva samostatné útoky sa zamerali na 50 000 rôznych používateľov Teams s cieľom phishingu na kontá Office 365**
- **Francúzsky denník Le Figaro odhalil vo forme API logov zhruba 7,4 miliárd záznamov obsahujúcich informácie (mená, heslá, telefónne čísla, adresy,...) umožňujúce identifikáciu ich reportérov a zamestnancov, ako aj najmenej 42 000 používateľov**
- **Na vysoko postavených zamestnancov zo Severnej Ameriky ale aj iných častí sveta, bol použitý sofistikovaný phishingový email. Analytici sa domnievajú, že existuje najmenej 150 obetí**
- **Útočníci tvrdia, že odcudzili údaje 11 miliónov kreditných kariet a iných informácií zo siete Banco BCR, národnej banky Kostariky**
- **Novoobjavená vzorka škodlivého softvéru „EventBot" pre Android je zameraná na používateľov takmer 300 finančných aplikácií v USA a Európe**

- **Cerberus už nie je jednoduchým malvérom pre Android. Vyvinul sa na RAT, ktorý môže prevziať úplnú kontrolu nad zariadeniami a automaticky sa šíriť prostredníctvom serverov mobilných zariadení**

- **Útočník zverejnil údaje o 15 miliónoch používateľov zaregistrovaných v najväčšom indonézskom internetovom obchode Tokopedia**

- **Údaje 44 miliónov pakistanských mobilných používateľov boli zverejnené online po tom, čo sa útočník pokúsil minulý mesiac predať balík obsahujúci 115 miliónov takýchto záznamov mobilných používateľov za bitcoiny vo výške 2,1 milióna dolárov**

- **Vedci varujú pred pokračujúcim phishingovým útokom, v ktorom útočníci napodobňujú známu telekomunikačnú spoločnosť EE, aby získali údaje a podrobnosti o platbách od vedúcich pracovníkov spoločností**

- **Z webovej stránky CAM4 na živé vysielanie pre dospelých unikli súkromné chaty, emaily, mená, emailové adresy používateľov, hashe hesiel, adresy IP a ďalšie informácie**

- **Nová phishingová kampaň sa zameriava na investičných maklérov pomocou podvodných emailov zameraných na odcudzenie poverení v aplikáciách Microsoft SharePoint a Office**

- **Phishingové útoky využívajú falošné upozornenia na chyby certifikátov s grafikou a formátovaním, ktoré boli stiahnuté z e-mailov spoločnosti Cisco Webex, aby ukradli údaje z účtov používateľov**

- **Pokročilí útočníci známi od roku 2010, vyvinuli nový backdoor malvér „Aria-body“**

- **Nigérijskí počítačoví útočníci, ktorí sa špecializovali na kompromitáciu obchodných emailov, využívali ako návnadu COVID-19 pri nedávnych útokoch na zdravotnícke a vládne organizácie**

- **Agentúra US Marshals Service (USMS) sa stala minulý rok obeťou prieniku a v súčasnosti oznamuje viac ako 387 000 väzňom, že pri incidente mohli byť ukradnuté ich osobné údaje**

- **Útočníci ukryli malvér v legitímnej dvojfaktorovej autentifikačnej aplikácii (2FA) pre macOS na distribúciu Dacls, trójskeho koňa so vzdialeným prístupom spojeného so skupinou Lazarus v Severnej Kórei**

- **Výrobca bankomatov Diebold Nixdorf potvrdil, že bol nedávno zasiahnutý ransomvérom, ale spoločnosť uviedla, že incident spôsobil iba „obmedzený výpadok IT systémov“**

- **Databáza zaniknutého fóra hackerov a trh pre úniky údajov s názvom WeLeakData.com sa predáva na dark webe a odhaľuje súkromné rozhovory útočníkov, ktorí stránku používali**

- **Irán ohlásil neúspešný kybernetický útok na prístav v prielive Hormuz. Iránski predstavitelia uviedli, že útočníci poškodili malý počet počítačov v prístave Šahid Rajaei v meste Bandar Abbas**

- **Spoločnosť ESET bola nútená čeliť útoku DDoS pochádzajúcemu od škodlivej spravodajskej aplikácie z obchodu Google Play, ktorá bola stiahnutá najmenej 50 000-krát**

- **Bezpečnostný analytik zozbieral v priebehu niekoľkých týždňov viac ako 1 000 domén infikovaných skimmermi platobných kariet, čo dokazuje, že MageCart je naďalej prevládajúcou hrozbou**

- **APT skupina čínskych hackerov Naikon ukrývala päť rokov internetovú špionáž zameranú na vládne subjekty**

- **Ruhr University Bochum (RUB) oznámila, že po ransomvérový útoku musela vypnúť veľkú časť svojej IT infraštruktúry vrátane zálohovacích systémov**

- **Najväčší súkromný prevádzkovateľ nemocníc, Fresenius, bol napadnutý ransomvérom**

- **Na hackerskom fóre sa našli prihlasovacie údaje používateľov zoznamovacej aplikácie Mobifriends**

- **Právne dokumenty celebrít boli odcudzené pri útoku ransomvéru REvil na prominentnú advokátsku kanceláriu**

- **Webhostingová spoločnosť Digital Ocean neúmyselne zverejnila niektoré údaje zákazníkov na internete**

- **Výrobca železničných vozidiel Stadler bol zasiahnutý kybernetickým útokom**

- Spoločnosť Magellan Health Inc oznámila, že sa stala obeťou útoku ransomvéru, čo videlo k odcudzeniu osobných údajov z jedného z jej serverov
- Globálna spoločnosť Pitney Bowes zastavila útok ransomvéru Maze skôr, ako boli zašifrované dáta, avšak útočníkom sa podarilo ukradnúť niektoré údaje
- Viac ako 4000 aplikáciám pre Android unikajú údaje používateľov prostredníctvom nesprávne nakonfigurovaných databáz Firebase
- Britský sprostredkovateľ elektriny Elexon bol zasiahnutý kybernetickým útokom
- Niekoľko superpočítačov naprieč Európou bolo vypnutých po tom, čo boli cieľom kampane na ťažbu kryptomien
- Malvér WolfRAT sa zameriava na používateľov aplikácií WhatsApp a Facebook Messenger na zariadeniach s operačným systémom Android
- Ukrajinskej polícii sa podarilo zatknúť útočníka, ktorý predával miliardy ukradnutých záznamov
- Tisíce izraelských webov boli zasiahnuté koordinovaným kybernetickým útokom
- Japonsko vyšetruje možný únik údajov vrátane podrobností o prototype rakety pri masívnom kybernetickom útoku na spoločnosť Mitsubishi Electric Corp
- Inteligentný phishingový útok obchádza viacfaktorovú autentifikáciu aby ukradol prihlasovacie údaje do Microsoft Office 365
- Útočník zverejnil viac ako 40 miliónov záznamov používateľov aplikácie Wishbone zadarmo
- Spoločnostiam Qihoo a Baidu sa podarilo znefunkčniť botnet, ktorý infikoval stovky tisíc počítačov
- 25 miliónov používateľských záznamov uniklo z populárnej matematickej aplikácie Mathway
- Pomocou útoku ransomvérom bola napadnutá sieť Michiganskej štátnej univerzity
- Kyberzločinci predávajú údaje 26 miliónov používateľov LiveJournal na dark webe

- **Servery Microsoft IIS boli napadnuté skupinou Blue Mockingbird za účelom ťažby kryptomeny Monero**

- **Americká Národná bezpečnostná agentúra (NSA) zverejnila varovanie pred novou vlnou kybernetických útokov voči emailovým serverom Exim, ktoré sú vedené jednou z pokročilých kybernetických špionážnych jednotiek v Rusku**

Závažné zraniteľnosti bežných softvérových produktov

Zero-day zraniteľnosť aplikácie Zoom pre Windows umožňuje šírenie malvéru a vykonávanie kódu

V aplikácii Zoom zameriavajúcej sa na video konferenčné hovory bola nájdená kritická zeroday zraniteľnosť. Nachádza sa v klientovi aplikácie na operačnom systéme Windows. Táto zraniteľnosť vzniká v spôsobe akým aplikácia spracováva Uniform Resource Identifier (URI) cesty a jej zneužitie umožňuje útočníkovi vzdialené vykonávanie kódu. Po zneužití zraniteľnosti môže útočník získať informácie o sieti alebo tiež vykonať útok UNC injection (Universal Naming Convention).

Cisco opravilo kritické zraniteľnosti vo viacerých produktoch

Spoločnosť Cisco vydala bezpečnostné záplaty na kritické a závažné zraniteľnosti viacerých produktov. Vzdialený útočník mohol tieto zraniteľnosti využiť so zámerom získať kontrolu nad postihnutým systémom, vykonávať kód, či spôsobiť nedostupnosť služby. Americká vládna agentúra CISA nabáda užívateľov a administrátorov, aby zraniteľné systémy bezodkladne aktualizovali.

Spoločnosť Juniper vydala bezpečnostné aktualizácie pre Junos OS

Spoločnosť Juniper vydala bezpečnostné aktualizácie na opravu zraniteľnosti, ktorá ovplyvňovala viaceré verzie operačného systému Junos. Túto chybu mohol útočník zneužiť na prevzatie kontroly nad zraniteľným systémom. Útočníkom to tiež umožňovalo vzdialene vykonávať kód, obísť bezpečnostné obmedzenia a prístup k citlivým informáciám zo systému. Táto zraniteľnosť sa týka iba zariadení s OS Junos s povolenými službami HTTP/HTTPS.

Protokol Samba – bezpečnostné aktualizácie pre viaceré verzie

Tím Samba vydal bezpečnostné aktualizácie opravujúce 2 zraniteľnosti týkajúce sa protokolu LDAP. Zneužitie týchto zraniteľností môže umožniť prístup ku odalokovanému miestu v pamäti a tiež narušenie dostupnosti systému. Na opravu týchto zraniteľností boli vydané nové verzie Samba 4.10.15, 4.11.8 a 4.12.2.

Bezpečnostná chyba v MS Teams umožňuje prevzatie kontroly nad účtom

Bezpečnostná zraniteľnosť, nájdená v spôsobe načítania obrázkov GIF a overenia doručenia tohto typu súboru, umožňuje prebrať plnú kontrolu nad napadnutým účtom. Dochádza k tomu prostredníctvom obídenia autentifikácie API rozhrania MS Teams použitím dvoch získaných autentifikačných tokenov. Zraniteľnosť môže byť zneužitá v desktopovej aj webovej verzii aplikácie.

Spoločnosť Cisco odstránila závažnú zraniteľnosť na IOS XE SD-WAN Software

Spoločnosť Cisco vydala bezpečnostnú záplatu na zraniteľnosť v Command Line Interface (CLI) systému Cisco IOS XE SD-WAN. Zraniteľnosť umožňuje overenému lokálnemu útočníkovi vykonať injekciu ľubovoľného príkazu, ktorý je realizovaný s právami ROOT. Bezpečnostná chyba je spôsobená nedostatočným overovaním príkazov na vstupe. Útočník môže zneužiť túto zraniteľnosť tak, že sa autentifikuje voči zariadeniu a vloží špeciálne upravený obsah do Command Line Interface CLI.

Spoločnosť VMware vydala bezpečnostnú opravu XSS zraniteľnosti

Spoločnosť VMware vydala bezpečnostnú opravu zraniteľnosti XSS (cross-site scripting) s vysokou závažnosťou v produkte VMware ESXi. Zraniteľnosť CVE-2020-3955 bola popísaná v bezpečnostnom odporúčaní VMSA-2020-0008 vydanom na oficiálnej stránke VMware. Ovplyvňuje verzie VMware ESXi 6.5 a 6.7. Zverejnená zraniteľnosť umožňuje útočníkovi vzdialene vykonať HTML kód alebo skript na zraniteľnej webstránke.

Spoločnosť SaltStack opravila kritické zraniteľnosti v softvéri Salt

Spoločnosť SaltStack vydala aktualizáciu, ktorá sa zameriava na opravu kritických zraniteľností ovplyvňujúcich verzie Salt staršie ako 2019.2.4 a 3000.2. Vzdialený útočník by tieto zraniteľnosti mohol zneužiť okrem iného na prevzatie kontroly nad postihnutým systémom. Niekoľko dní po vydaní varovaní sa útočníkom podarilo zneužiť tieto zraniteľnosti a napadnúť dve organizácie využívajúce technológiu SaltStack.

Kritická zero-click zraniteľnosť Samsungu v systéme Android verzie 8, 9 a 10

V OS Android používanom spoločnosťou Samsung bola objavená kritická bezpečnostná chyba súvisiaca so spracovaním obrázkového formátu Qmage, ktorá umožňuje úplnú kompromitáciu zariadenia pomocou MMS správ. Jej zneužitie nevyžaduje od obete žiadnu interakciu.

BIAS – kritická zraniteľnosť v protokole Bluetooth

Vo všetkých zariadeniach využívajúcich protokol Bluetooth BR/EDR sa nachádza bezpečnostná zraniteľnosť, ktorá umožňuje krádež identity už spárovaného zariadenia. Útočník sa môže bez ďalšieho overovania pripojiť na hostiteľské zariadenie.

Päť zero-day zraniteľností vo Windows umožňuje získať vyššie práva

Bezpečnostní experti spoločnosti Trend Micro Zero Day Initiative (ZDI) zverejnili informácie o piatich zneužívaných zraniteľnostiach operačného systému Windows, na ktoré zatiaľ neexistujú záplaty. Útočník by ich mohol zneužiť pre získanie vyšších používateľských oprávnení na postihnutom systéme. Tieto bezpečnostné chyby boli identifikované v hostiteľskom procese splwow64.exe pre tlačiarenské ovládače a sú spôsobené nesprávnym overovaním vstupných hodnôt zadávaných používateľom.

Zraniteľnosť open source webového redakčného systému Drupal

V redakčnom systéme Drupal core boli nájdené 2 závažné zraniteľnosti. Jednou je zraniteľnosť typu XSS, ktorá súvisí s dvomi zraniteľnosťami v JavaScript knižnici jQuery, druhou je zraniteľnosť typu Open redirect v Drupal 7, ktoré umožňujú podvrhnúť súčasti stránky, alebo samotnú web stránku.

TLP: White

Zraniteľnosti VMware

V produktoch VMWare bola opravená 1 závažná zraniteľnosť:
CVE-2020-3956: Overený používateľ môže odoslať škodlivú komunikáciu do VMware Cloud Director, čo môže viesť k svojvoľnému vzdialenému vykonaniu kódu. Túto zraniteľnosť možno zneužiť prostredníctvom používateľských rozhraní založených na HTML5 a Flex.

Zraniteľnosti Intel

V produktoch Intel neboli opravené žiadne kritické ani závažné zraniteľnosti.

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Adaptive Security Appliance Software CVE-2020-3125: Aplikácia je náchylná na kritickú zraniteľnosť adresára kvôli nedostatočnej validácii vstupu dodávaného používateľom do rozhrania postihnutého zariadenia. Tento problém sa týka konkrétne autentifikácie Kerberos.
Cisco AMP for Endpoints Mac Connector CVE-2020-3314: Aplikácia je náchylná na zraniteľnosť umožňujúcu DoS (odmietnutie služby) z dôvodu nedostatočného overenia vstupu určitých atribútov súborov.
Cisco Unified Contact Center Express CVE-2020-3280: Zraniteľnosť vzniká pri spustení kódu v aplikácii z dôvodu nedostatočne zabezpečenej deserializácie obsahu dodávaného používateľom.
Cisco ASA Software and FTD Software CVE-2020-3195, CVE-2020-3254, CVE-2020-3303: Závažné zraniteľnosti v produktoch Cisco ASA a FTD Software môžu po zneužití spôsobiť zraniteľnosť DoS (odmietnutie služby).
Cisco Firepower Management Center CVE-2020-3311: Produkt je náchylný na zraniteľnosť presmerovania, pretože nedokáže správne overiť parametre v požiadavke HTTP. Tento problém sa týka najmä webového rozhrania pre správu systému.

TLP: White

Cisco Firepower Management Center CVE-2020-3313: Kvôli nedostatočnému overovaniu vstupov od používateľov je v produktoch umožnené zneužitie zraniteľností typu XSS.
Cisco Umbrella CVE-2020-3246: Webový server Cisco Umbrella je náchylný na zraniteľnosť CRLF-injekcie kvôli nedostatočnému overovaniu vstupu používateľa.
Cisco AsyncOS Software CVE-2020-3178: Kvôli neschopnosti overovania parametrov požiadavky HTTP, je Cisco AsyncOS Software náchylný na chybu zabezpečenia presmerovania. Tento problém sa týka najmä webového rozhrania pre správu systému.

Mesačník zraniteľností Máj 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
    - Zero-day zraniteľnosť aplikácie Zoom umožňuje šírenie malvéru a vykonávanie kódu
    - Cisco opravilo kritické zraniteľnosti vo viacerých produktoch
    - Spoločnosť Juniper vydala bezpečnostné aktualizácie pre Junos OS
    - Protokol Samba – bezpečnostné aktualizácie pre viaceré verzie
    - Bezpečnostná chyba v MS Teams umožňuje prevzatie kontroly nad účtom
    - Spoločnosť Cisco odstránila závažnú zraniteľnosť na IOS XE SD-WAN Software
    - Spoločnosť VMware vydala bezpečnostnú opravu XSS zraniteľnosti
    - Spoločnosť SaltStack opravila kritické zraniteľnosti v softvéri Salt
    - Kritická zero-click zraniteľnosť Samsungu v systéme Android verzie 8, 9 a 10
    - BIAS – kritická zraniteľnosť v protokole Bluetooth
    - Päť zero-day zraniteľností vo Windows umožňuje získať vyššie práva
    - Zraniteľnosť open-source webového redakčného systému Drupal

https://www.csirt.gov.sk/aktualne-7d7.html?id=216