MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK
Jún 2020

Vypracoval: CSIRT.SK

TLP: White

Takmer pred rokom sme v mesačnej správe spomínali tzv. APT skupiny, označujúce skupiny útočníkov, ktoré štandardne platí a organizuje konkrétny štát. Ich najčastejšou motiváciou je získanie vojenských a politických tajomstiev iných štátov, či ich technológií a poznatkov. Najznámejšie skupiny pracujú pre Rusko, Čínu, Irán, Severnú Kóreu, Saudskú Arábiu, Izrael, či štáty Five Eyes (USA, Kanada, Veľká Británia, Austrália, Nový Zéland). Útoky takejto skupiny boli nedávno zaznamenané aj na našom území, pričom cieľom sa stali dve slovenské spoločnosti. Okrem Slovenskej republiky boli cieľom Južná Kórea, Veľká Británia, USA, Turecko či Ukrajina.

Útok, ktorý zasiahol aj územie Slovenskej republiky, pochádzal zo Severnej Kórei a jeho cieľom bol sektor dodávateľov zbraní. Útočníkom bola severokórejská skupina APT38 RGB-D3, taktiež nazývaná aj Lazarus Group. Táto skupina stojí aj za pravdepodobne najznámejším ransomvérovým útokom WannaCry, ktorý sa odohral v roku 2017. Kým Lazarus sa zameriava hlavne na letecké a obranné spoločnosti, ich podskupina APT38 RGB-D5, nazývaná Kimsuky, sa zameriava hlavne na spoločnosti delostreleckej munície a vojenských vozidiel. Nedávny útok skupiny APT38 bol odhalený spoločnosťou ESET koncom minulého roka. Len na základe známych operácií sa skupina pokúsila ukradnúť viac ako 1,1 miliardy dolárov.

Pri danom útoku sa škodlivý kód k vybraným, prevažne leteckým spoločnostiam dostal v podobe súboru. Zamestnanci daných spoločností boli útočníkmi kontaktovaní na portáli LinkedIn pomocou falošného profilu. Pomocou súkromnej správy, navrhol tento falošný profil zamestnancovi pracovnú ponuku v jeho spoločnosti. V prípadoch, ktoré boli odhalené, sa útočníci zamestnancom predstavovali ako zástupcovia známych spoločností v leteckom a obrannom priemysle. Po nadviazaní kontaktu s obeťou, podsunuli útočníci do komunikácie škodlivé súbory a maskovali ich ako dokumenty súvisiace s inzerovanou pracovnou ponukou. Zamestnancovi tak do správy mohol prísť napríklad PDF dokument so spísanými pracovnými pozíciami a prislúchajúcimi ročnými platmi.

Súbory boli obetiam poslané priamo cez komunikáciu na portáli LinkedIn alebo pomocou odkazu na úložisko OneDrive. Odkaz do počítača stiahol zaheslovaný archív RAR, ktorý pomocou súboru LNK následne stiahol spomínaný dokument. Tento dokument slúžil ako návnada, pri jeho stiahnutí sa totiž na pozadí vykonali príkazy potrebné na zaistenie perzistencie na kompromitovanom počítači.

Po počiatočnom vniknutí útočníci preskúmali prostredie počítača pomocou príkazov PowerShell. Týmito príkazmi si v počítači zabezpečili napríklad aj obranu proti detekcii či získali zoznam zamestnancov, vrátane správcovských účtov. To im následne umožnilo vykonať útok hrubou silou na tieto účty. Zjavným cieľom útoku sú teda údaje o danej spoločnosti, v niektorých prípadoch sa útočníci takisto pokúsili speňažiť prístup k emailovému účtu obete.

APT38 je skupina útočníkov, ktorá je orientovaná finančne. Podľa známych prípadov je táto skupina zodpovedná za viacero útokov voči finančným inštitúciám, ako aj za niektoré z najväčších počítačových lúpeží vôbec (útok WannaCry). Existuje mnoho podobností medzi APT38 a TEMP.Hermit, severokórejskou špionážnou skupinou. Podobnosti medzi škodlivými kódmi, ktoré tieto skupiny

používajú naznačujú istú spoluprácu. APT38 už od roku 2014 vykonáva sofistikované bankové, ale aj iné lúpeže, ktoré zvyčajne zahŕňajú dlhé plánovanie a prípravu. Medzi ich známe útoky patrí napríklad pokus o lúpež v TPBank, Bangladéšskej banke, Far Eastern International na Taiwane či Banco de Chile. Aktivity skupiny APT38 začali vo februári 2014 a pravdepodobne boli motivované finančnými sankciami prijatými voči Severnej Kórei v marci 2013, ktoré blokovali hromadné prevody hotovosti a obmedzovali prístup Severnej Kórey do medzinárodných bankových systémov.

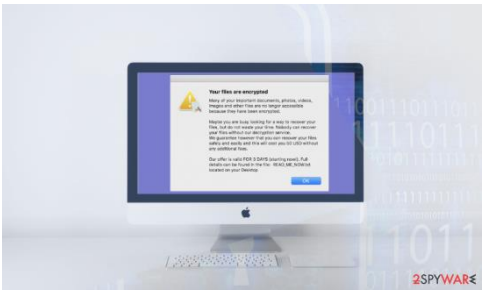
Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci jún riešil štandardne najmä phishingové kampane na svoju konštituenciu. Okrem toho CSIRT.SK vykonal forenznú analýzu PC napadnutom malvérom Agent Tesla, pričom došlo k úniku prihlasovacích údajov ku niekoľkým účtom obete. Boli zaistené vzorky malvéru a vydané odporúčania pre zamedzenie prístupu útočníkov ku predmetným účtom a opätovnej infekcie kompromitovaného zariadenia.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK varovala svoju konštituenciu pred šírením škodlivých falošných aktualizácií internetových prehliadačov Google Chrome a Mozilla Firefox. Jednalo sa o kampaň APT skupiny Lazarus. Upozornila aj na ďalšie kampane tejto skupiny. V jednej ako návnada figurovala falošná pracovná ponuka od spoločnosti Disney, v druhej sa skupina skrývala za falošné pracovné ponuky niekoľkých firiem zo sektoru obrany a letectva. CSIRT.SK s varovaniami poskytol aj indikátory kompromitácia, vrátane škodlivých domén a hašov súborov.
CSIRT.SK začal v rámci svojej konštituencii vykonávať kontroly využívania technológií zabezpečenia e-mailovej komunikácie, SPF a DKIM. Jednotka rozposlala odporúčanie pre nasadenie týchto prvkov.

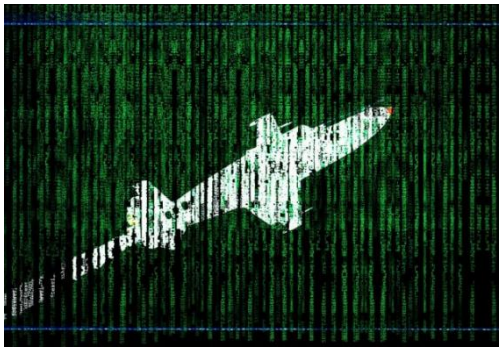
Významné útoky vo svete

Nový ransomvér ThiefQuest napáda zariadenia s operačným systémom macOS



Ransomvér s názvom ThiefQuest sa od väčšiny odlišuje tým, že okrem šifrovania súborov monitoruje aj klávesnicu, dokáže ukradnúť peňaženky kryptomien a umožniť útočníkovi získať kontrolu nad napadnutým systémom. Okrem toho má vlastnosti na zabránenie jeho analýzy a zabezpečenie perzistencie. Ransomvér bol distribuovaný cez nelegálne šírený softvér na BitTorrent stránkach. Po zašifrovaní sa vytvoril súbor s inštrukciami na zaplatenie. V zachytených vzorkách bolo požadovaných 50 dolárov. Aby sa zabezpečilo, že si obeť všimne požiadavku na výkupné, ransomvér spustil požiadavku na čítanie textu s využitím hlasovej možnosti systému macOS.

Špionážna kampaň bola namierená na letecké a vojenské spoločnosti



Operation In(ter)ception je špionážna kampaň zameraná na letecké a vojenské spoločnosti v Európe a na Strednom Východe. Kampaň zachytila spoločnosť ESET, podľa ktorej okrem špionáže išlo aj o získanie peňazí pomocou kompromitovaných emailových adries. ESET podozrieva Lazarus group, skupinu útočníkov pracujúcu pre Severnú Kóreu. Kampaň začínala sociálnym inžinierstvom pomocou ktorého útočníci lákali na falošné pracovné ponuky cez LinkedIn. Počas komunikácie poslali útočníci obetiam súbory, ktoré mali obsahovať detailnejšie informácie o pracovných ponukách. Súbor vzdialene spúšťal skript, vďaka ktorému sa útočníci dostali do počítača a stiahli zadné vrátka, ktoré komunikujú s riadiacim serverom a posielajú mu získané informácie.

UCSF zaplatila 1,14 milióna dolárov útočníkom

Skupina útočníkov s menom Netwalker Ransom Operators sa zacielila na vysoké školy v spojených štátoch. V máji oznámili, že zašifrovali dáta Michigan State University a zverejnili ich malú časť s hrozbou ich zverejnenia, ak nedostanú výkupné. Univerzita výkupné nezaplatila, a útočníci dáta zverejnili. Neskôr publikovali vzorku uniknutých súborov z University of California San Francisco (UCSF) s rovnakou hrozbou. Tie obsahovali osobné údaje študentov a zamestnancov. Univerzita tvrdí, že útok zasiahol len niektoré medicínske systémy a starostlivosť o pacientov nie je ohrozená. Napriek tomu sa rozhodli útočníkom zaplatiť 1,14 milióna USD.

Skupina stojaca za REvil ransomvérom spustila aukciu ukradnutých dát

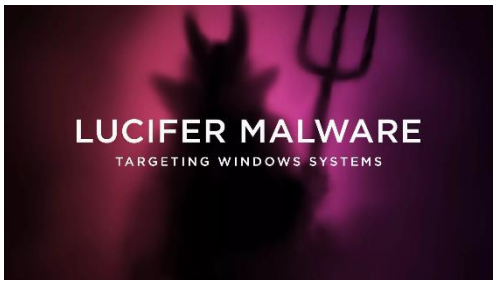
Skupina REvil spustila aukciu, v ktorej predáva dáta získané zo spoločností, ktoré boli obeťami jej útokov. Ceny položiek v aukcii sa pohybujú od desiatok tisíc až po milióny dolárov. Okrem osobných údajov zamestnancov a zákazníkov predávali aj dáta týkajúce sa intelektuálneho vlastníctva, ako napríklad nové technológie a nezapísané patenty. Aukcie sú úplne anonymné. Účastníci dostanú jednorazové prístupové údaje a adresy na unikátne krypto peňaženky.

Evil Corp útočí s ransomvérom WastedLocker

Skupina Evil Corp útočí s novým ransomvérom WastedLocker výlučne na spoločnosti v Spojených štátoch s požiadavkami na výkupné v miliónoch dolárov. Okrem šifrovania súborov kradnú aj prístupové údaje a snažia sa získať kontrolu nad zariadeniami obetí. Výskumníci zo Symantecu hovoria, že sa útočilo na minimálne 31 spoločností. Útoky boli prekazené skôr, ako prebehlo zašifrovanie súborov. Obete boli infikované cez napadnuté webstránky, z ktorých mnohé boli spravodajské.

TLP: White

Nový DDoS malvér Lucifer útočí na Windows systémy



Bezpečnostní experti identifikovali nový malvér Lucifer (pôvodne Satan) ktorý používa DDoS útoky, ťaží kryptomeny a dokáže sa sám šíriť. Malvér využíva veľké množstvo zraniteľností v snahe dostať sa do systému. Po tom, čo sa do systému nainštaluje, sa pripojí k riadiacemu serveru a je použitý na DoS útoky alebo ťažbu kryptomien. Okrem toho skenuje otvorené porty, cez ktoré sa kopíruje po sieti. Malvér má tiež schopnosti na zabránenie jeho analýzy a detekcie.

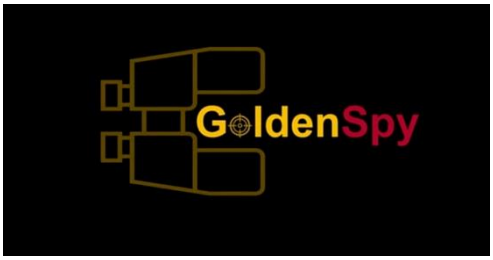
Skupina útočníkov zverejnila BlueLeaks, zbierku súborov ukradnutých z viac ako 200 policajných oddelení

Skupina DDoSecret, ktorá sa prezentuje ako transparentnejšia alternatíva WikiLeaks, publikovala 269 GB dát polície. Podľa skupiny útočníkov obsahujú policajné a FBI správy, príručky, emaily a iné informácie za posledných 24 rokov. Obsahujú aj osobné informácie ako IBAN, telefónne čísla, emailové adresy, fotky a iné informácie ktoré umožňujú identifikáciu osôb. Spolu uniklo viac ako milión súborov. Skupina tvrdí, že dáta dostala od hackerskej skupiny Anonymous. Podľa analýzy z National Fusion Center Association (NFCA) boli údaje získané z úniku dát spoločnosti Nestsential ktorá poskytuje web-hosting.

Na Austrálsku vládu pravdepodobne útočil iný štát

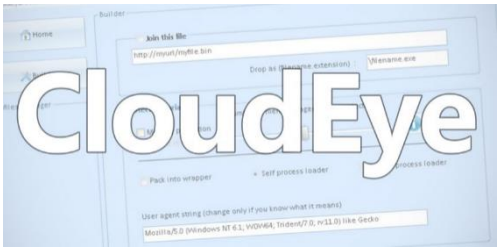
Austrálsky premiér na tlačovej konferencii povedal, že jeho krajina bola pod rozsiahlym kybernetickým útokom ktorý bol cielený na vládu, austrálske spoločnosti a kritickú infraštruktúru. Vzhľadom na sofistikovanosť a rozsah útoku je podľa premiéra podozrivý iný štát. Pri útoku bol použitý malvér, ktorý využívajú čínske hackerské skupiny a uniknutý kód iránskej skupiny. Austrália reagovala zvýšením financií na kybernetickú bezpečnosť krajiny na nasledujúcu dekádu o 1,35 miliárd austrálskych dolárov.

V čínskom daňovom softvéri sa nachádzal malvér



Dve softvérové spoločnosti z Veľkej Británie boli napadnuté novým malvérom s názvom GoldenSpy. Malvér sa nachádzal v daňovom softvéri, ktorého inštaláciu od nich požadovala lokálna čínska banka. Softvér vytvorila čínska spoločnosť Aisino Corporation. Obsahoval zadné vrátka, ktoré umožnili útočníkovi pripojiť sa s administrátorskými oprávneniami. Malvér je perzistentný a neodinštaluje sa spolu s daňovým softvérom. Krátko po publikovaní odhalení si nainštalovaný softvér stiahol súbor, ktorý odstránil GoldenSpy a zahladil všetky stopy jeho použitia. Momentálne nie je jasné, kto pribalil malvér k daňovému softvéru, ani kto ho využíval.

Talianska spoločnosť je podozrivá z pridávania škodlivých funkcií do svojho produktu



Talianska spoločnosť CloudEye predáva produkt CloudEye Protector, ktorý má slúžiť ako šifrovací program a chrániť softvér pred reverzným inžinierstvom. Výskumníci z Check Point tvrdia, že tento produkt obsahoval malvér GuLoader ktorý slúži na sťahovanie ďalšieho škodlivého kódu. Protector tiež obsahoval funkcionality, ktoré sú podľa výskumníkov špecificky navrhnuté na podporu GuLoadera. Výskumníci tiež zistili, že v minulosti táto spoločnosť propagovala produkt DarkEye ktorý mal slúžiť na šifrovanie malvéru. Jedno z emailových kont použitých na propagáciu DarkEye má patriť spoluzakladateľovi CloudEye. Emailové kontá spojené s CloudEye boli použité aj na kyber-kriminálnych fórach, kde propagovali služby šifrovania malvéru už v roku 2011.

Spoločnosť, ktorá Nemeckej vláde dodávala ochranné vybavenie bola cieľom phishingovej kampane

Bezpečnostní experti zo spoločnosti IBM varujú pred stále trvajúcou cielenou phishingovou kampaňou, ktorá je zameraná na spoločnosť dodávajúcu ochranné vybavenie v súvislosti s pandémiou COVID-19 nemeckej vláde. Kampaň začala už v marci a doteraz bolo jej cieľom viac ako 100 vedúcich zamestnancov spoločnosti a jej partnerov. Vo phishingových emailoch sa nachádzali odkazy na stránky, ktoré sa kamuflovali ako prihlasovacie stránky Microsoftu a získané údaje

posielali na emailové kontá spoločnosti Yandex. Experti túto kampaň vysledovali až k ruskej IP adrese a notifikovali nemecký CERT.

Útočníci napadli sektor služieb v Spojených štátoch amerických

Malvér typu RAT známy ako FlowCloud používaný v kampaniach proti sektoru služieb bol pravdepodobne zneužitý rovnakým útočníkom ktorý použil LookBack malvér. V oboch kampaniach boli použité témy tréningu a certifikácie pri phishingu, používali rovnaké makrá v prílohách a obe rodiny malvéru používajú rovnaké inštalačné techniky. V oboch skupinách kampaní sa prelínali ciele - spoločnosti aj osoby. Útočník označený ako TA410 použil podobné techniky ako boli použité v čínskych kampaniach skupiny APT10. Malvér FlowCloud dokáže ovládať klávesnicu, myš a obrazovku, tiež vie manipulovať so súbormi a procesmi v počítači. Získané informácie posiela na riadiaci server.

Dodávateľ nukleárnych rakiet pre USA bol zasiahnutých ransomvérom

Nukleárny dodávateľ Westech International potvrdil, že jeho sieť bola prelomená a jeho počítače sú zašifrované ransomvérom s názvom Maze. Útočníci požadujú výkupné a zverejnili citlivé informácie, ako napríklad emaily a výplatné pásky. V prípade, že výkupné nebude zaplatené, chcú zverejniť všetky dáta ktoré získali pri útoku. Nie je jasné, či útočníci získali utajené vojenské informácie. Westech sa doposiaľ nevyjadril k výške výkupného, ani k tomu, či ho chce zaplatiť.

- **Phishingová kampaň sa zameriava na vlastníkov webstránok pomocou emailov, ktoré predstierajú, že pochádzajú od prevádzkovateľa hostingu**
- **Skimmery platobných kariet Magecart boli nájdené na webových stránkach ôsmich miest v Spojených štátoch**
- **Niektoré Docker image obsahujú malvér Monero určený na ťažbu kryptomien**

- **Malvér s názvom AcidBox využíva exploit prepojený s ruskou APT skupinou Turla**
- **Skupina útočníkov InvisiMole sa zameriava na diplomatické misie a významné organizácie vo vojenskom sektore**
- **V USA sa objavil phishingový útok obchádzajúci emailové ochrany, v ktorom sa útočníci vydávajú za Bank of America**
- **Poľskí výskumníci z oblasti kybernetickej bezpečnosti sledujú útoky ransomvéru s názvom Black Kingdom, ktorý využíva zraniteľnosť Pulse Secure VPN**
- **Mesto Knoxville muselo vypnúť svoju sieť po útoku ransomvérom**
- **Phishingová emailová kampaň, ktorá žiada o anonymné hlasovanie k hnutiu Black Lives Matter šíri malvér Trickbot určený na kradnutie údajov**
- **Ransomvér Thanos ako prvý využíva techniku s názvom RIPlace, čo mu umožňuje obísť ochranu proti ransomvérom systému Windows**
- **Európska energetická spoločnosť Enel Group bola zasiahnutá ransomvérom s názvom Snake**
- **Počítačové siete spoločnosti Honda v Európe a Japonsku boli zasiahnuté kybernetickým útokom**
- **Skupina útočníkov Dark Basin pod záštitou indickej IT spoločnosti útočila v posledných rokoch na tisíce organizácií a jednotlivcov vrátane novinárov a politikov**
- **Výroba v Austrálskej spoločnosti s nápojmi Lion bola prerušená kvôli ransomvéru**
- **Najväčší poskytovateľ internetu v Rakúsku bol napadnutý malvérom, ktorého odstraňovanie trvalo 5 mesiacov**
- **Botnet Kingminer sa hrubou silou snaží dostať do MSSQL databáz na ktorých potom ťaží kryptomenu**
- **Ransomvér Avaddon využíva 28 rokov staré makrá Excel 4.0, ktoré je náročné analyzovať**
- **Spoločnosť Conduent bola zasiahnutá ransomvérom Maze**

- **Spoločnosti Xerox hrozí, že skupina ktorá ju napadla ransomvérom Maze zverejní 100 GB dát ak nedostane výkupné**

- **Kampane Trumpa a Bidena sú zatiaľ neúspešne cieľom útočníkov z Číny a Iránu**

- **Útočníci sa neúspešne pokúsili získať konfigurácie a prístupové údaje na viac ako 1.3 milióna stránok WordPress prostredníctvom starých zraniteľností**

- **Hacker zverejnil databázu používateľov ukradnutú od poskytovateľa Daniel's Hosting, ktorá môže obsahovať informácie o kybernetických útočníkoch**

- **Octopus skener, ktorý cieli na NetBeans Java IDE bol odhalený v 26 repozitároch GitHub**

- **Ransomvér Tycoon sa v snahe uniknúť detekcii kompiluje do Java formátu JIMAGE, ktorý je na rozdiel od formátu JAR takmer nepoužívaný**

- **Malvér s názvom USBCulprit umožňuje ukradnúť dáta z izolovaných systémov a šíri sa cez USB médiá**

- **Výrobca čipov MaxLinear bol zasiahnutý ransomvérom Maze, ktorého operátori žiadajú výkupné aby nezverejnili získané osobné a finančné informácie**

- **Operátori ransomvéru s názvom eCh0raix spustili ďalšiu vlnu útokov voči QNAP NAS zariadeniam**

- **Uniknutá databáza systému Joomla obsahovala osobné informácie viac ako 2700 používateľov**

- **Spoločnosť National Railroad Passenger Corporation (Amtrak) potvrdila únik údajov, ktorý by mohol mať za následok ohrozenie osobných údajov zákazníka**

Závažné zraniteľnosti bežných softvérových produktov

Kritické zraniteľnosti v zariadeniach Cisco IOS / IOS XE

Spoločnosť Cisco oznámila, že opravila 25 kritických a závažných zraniteľností v routeroch využívajúcich operačný systém Cisco IOS / IOS XE. Tri najkritickejšie umožňujú obídenie autentifikácie, vykonávanie príkazov či vykonanie DoS útokov.

Zraniteľnosť v systéme Cisco NX-OS

V operačnom systéme sieťových prvkov NX-OS od spoločnosti Cisco bola nájdená zraniteľnosť, ktorá umožňuje obchádzať pravidlá konfigurované v zozname ACL, čo umožňuje kompromitáciu siete, alebo vykonanie DoS útoku. Útočník tiež získa možnosť preposielať svoje škodlivé pakety cez zraniteľné zariadenia a vykonávať tak DDoS útoky, či získavať informácie o ďalších obetiach.

Zraniteľnosť SMBleed protokolu Windows Server Message Block (SMBv3)

Spoločnosť ZecOps odhalila novú kritickú bezpečnostnú zraniteľnosť v dekompresnej funkcii SMBv3.1.1, v ktorej boli nedávno objavené aj zraniteľnosti SMBGhost a EternalDarkness. Zraniteľnosť dovoľuje únik citlivých dát, ktoré môžu byť ďalej zneužité na vzdialené vykonávanie kódu a kompromitáciu zraniteľného systému.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero rozličných kritických a závažných zraniteľností:
Intel AMT and ISM CVE-2020-0594, CVE-2020-0595: V dôsledku umožnenia čítania mimo hraníc môže nastať chyba zabezpečenia zvyšovania vzdialených privilégií.
Intel Solid State Drive CVE-2020-0527: Útočník môže v dôsledku nedostatočného riadenia toku údajov získať citlivé informácie zo

systému.
Intel Innovation Engine CVE-2020-8675: Nástroj je náchylný na zraniteľnosť spôsobenú lokálnymi oprávneniami kvôli nedostatočnému riadeniu toku údajov v nástroji na tvorbu a podpisovanie firmvéru.

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco Smart Software Manager On-Prem CVE-2020-3245: Pri spracúvaní špeciálnej HTTP požiadavky sa môže vyskytnúť chyba zabezpečenia neoprávneného prístupu.
Cisco Catalyst Switch CVE-2020-3231: Prepínače kvôli chybe umožňujú obídenie autentifikácie používateľa, pretože nedokážu správne spracovať údaje prenášané portom s povoleným rozhraním 802.1X.
Cisco IOS XE: V softvéri bolo opravených 25 kritických a závažných zraniteľností.

Mesačník zraniteľností Jún 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
    - Kritické zraniteľnosti v zariadeniach Cisco IOS / IOS XE
    - Zraniteľnosť v systéme Cisco NX-OS
    - Zraniteľnosť SMBleed protokolu Windows Server Message Block (SMBv3)

https://www.csirt.gov.sk/aktualne-7d7.html?id=218

TLP: White