MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

December 2020

Vypracoval: CSIRT.SK

TLP: White

Americká firma FireEye je jedna z najväčších svetových spoločností, ktoré sa zaoberajú kybernetickou bezpečnosťou. V mesiaci december utrpela útok na svoju infraštruktúru. Boli odcudzené penetračné nástroje, tzv. Red Team tools, ktoré spoločnosť využíva na testovanie bezpečnosti svojich zákazníkov. Použité techniky útočníkov nasvedčujú, že za útokom stojí skupina sponzorovaná štátom.

Ukradnuté nástroje zahŕňajú jednoduché skripty používané na automatizáciu, ale tiež celé rámce podobné verejne dostupným technológiám, ako sú CobaltStrike alebo Metasploit. Útočník tiež získal prístup k údajom o niektorých vládnych zákazníkoch, avšak neexistuje dôkaz, že by tieto údaje boli exfiltrované zo systémov. Spoločnosť na svojom GitHub účte zdieľa indikátory kompromitácie (IOC) a protiopatrenia na zmiernenie dopadov prípadného útoku. Spoločnosti na celom svete si tak môžu overiť, či ukradnuté nástroje spoločnosti FireEye neboli použité na narušenie ich sietí.

FireEye taktiež doposiaľ nezískala žiadny dôkaz o tom, že by útočníci zneužili ukradnuté nástroje. Použitím týchto nástrojov sú útočníci schopní kompromitovať systémy. Spoločnosť vyvinula viac ako 300 protiopatrení pre svojich zákazníkov a pre širokú komunitu, aby minimalizovali dopad krádeže. Nie je však známe, či útočníci chcú tieto nástroje použiť vo svoj prospech, alebo ich zverejniť. Predpokladá sa, že za útokom stojí ruská skupina APT29 (CozyBear). Rusko tieto obvinenia popiera.

O niekoľko dní neskôr spoločnosť SolarWinds oznámila narušenie platformy Orion, ktorú vyvíja. Tento nástroj slúži na bezpečnostné monitorovanie infraštruktúry organizácií, vrátane serverov, pracovných staníc, mobilných zariadení a zariadení IoT. Napadnuté boli aktualizácie platformy Orion verzie 2019.4 až 2020.2 HF 1, ktoré boli vydané od marca do júna 2020. Útok na spoločnosť FireEye tiež prebehol po tejto línii. Malvér, ktorý útočníci použili, nazvala SUNBURST. Spoločnosť Microsoft mu dala názvov Solorigate.

Medzi obete tohto malvéru patria americké federálne agentúry vrátane Ministerstva financií (US Treasury) a Amerického národného telekomunikačného a informačného úradu (US National Telecommunications and Information Administration). Predpokladá sa, že za týmito útokmi stojí rovnaká skupina, ako tá, ktorá ukradla nástroje spoločnosti FireEye. Produkty SolarWinds používa viac ako 300 tisíc zákazníkov na celom svete vrátane spoločností z rebríčka Fortune 500, vládnych agentúr a vzdelávacích inštitúcií. Využívajú ich tiež americké telekomunikačné spoločnosti, 5 zložiek americkej armády, Pentagón, Ministerstvo zahraničia USA, NASA a podobne.

Infikovaná verzia platformy okrem maskovania sieťového prenosu ako OIP protokol tiež komunikuje prostredníctvom protokolu http so vzdialenými servermi, aby mohol malvér prijímať a vykonávať škodlivé príkazy.

Spoločnosť SolarWinds verí, že skutočný počet zákazníkov, ktorí mohli mať nainštalovanú kompromitovanú verziu platformy Orion je menší ako 18 tisíc. Uviedla tiež, že sa od spoločnosti Microsoft dozvedela o kompromitácii svojich e-mailových účtov Office 365 a produkčných systémov.

Spoločnosť uviedla, že vyšetruje, či útočníci použili prístup k e-mailovým účtom na odcudzenie údajov o zákazníkoch. Tvrdí, že nenašla dôkazy o tom, že došlo k exfiltrácii údajov.

15. decembra sa spoločnosť Microsoft a koalícia technologických spoločností spojili s cieľom zmocniť sa domény avsvmcloud.com, ktorá slúžila ako riadiaci server. Samotný malvér po nainštalovaní ostáva nečinný 12 až 14 dní. Následne spustí príkaz ping na subdoménu avsvmcloud.com. Riadiaci server odpovie DNS odpoveďou, ktorá obsahuje pole CNAME s informáciami o inej doméne, odkiaľ má malvér SUNBURST získať ďalšie pokyny a užitočné dáta. Doména avsvmcloud.com sa v súčasnosti presmerováva na IP adresu vlastnenú spoločnosťou Microsoft.

Medzi primárne kroky na zmiernenie patrí inštalácia platformy Orion za brány firewall, zakázanie prístupu na internet pre platformu Orion a obmedzenie portov a pripojení iba na to, čo je nevyhnutné. Kompromitovaný súbor SolarWinds.Orion.Core.BusinessLayer.dll bol podpísaný legitímnym certifikátom. Verzie platformy Orion, ktoré boli kompromitované, majú tento súbor injektovaný malvérom. Preto je nutné v čo najkratšom čase aktualizovať na najnovšiu dostupnú verziu.

Spoločnosť SolarWinds žiada zákazníkov, aby aktualizovali platformu Orion na verzie 2019.4 HF 6 a 2020.2.1 HF 2, aby tak vylúčili akúkoľvek hrozbu. Microsoft uviedol, že Microsoft Defender začal umiestňovať do karantény škodlivé binárne súbory SolarWinds od 16. decembra. Označuje ich ako „Trojan:MSIL/Solorigate.BR!dha“. Odporúča, aby boli všetky servery, na ktorých je spustený softvér SolarWinds, izolované od zvyšku prostredia a pred ďalším uvedením do používania dôkladne vyšetrené na prítomnosť škodlivého softvéru.

Počas vyšetrovania tohto útoku spoločnosti Palo Alto Networks a Microsoft našli ďalší malvér s názvom SUPERNOVA, distribuovaný pomocou súboru App_Web_logoimagehandler.ashx.b6031896.dll. Slúži ako zadné vrátka, ktoré umožňujú útočníkom odoslať C# kód, ktorý by malvér skompiloval a spustil. Predpokladá sa, že tento malvér nesúvisí s predošlým. Znamená to však, že platforma Orion bola na distribúciu škodlivého softvéru použitá pri dvoch rôznych útokoch, pravdepodobne dvomi rôznymi skupinami.

Medzi napadnuté organizácie v rámci útoku na spoločnosť SolarWinds patria FireEye, U.S. Department of the Treasury, U.S. National Telecommunications and Information Administration (NTIA), U.S. Department of State, The National Institutes of Health (NIH) (Part of the U.S. Department of Health), U.S. Department of Homeland Security (DHS), U.S. Department of Energy (DOE), U.S. National Nuclear Security Administration (NNSA), niektoré americké štáty, Microsoft a Cisco.

Zoznam sa však stále môže rozširovať. Jedná sa o jeden z najrozsiahlejších kybernetických útokov vôbec. Spoločnosť Microsoft tiež identifikovala a informovala viac ako 40 svojich zákazníkov, ktorých sa tento útok týkal, ale nezverejnila ich mená. Uvádza, že 80% obetí bolo z USA. 44% bolo z IT sektoru, po 18% z vládneho sektoru a neziskoviek/think tankov, 9% bolo vládnych dodávateľov a 11% z ostatných sektorov.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci december riešil štandardne najmä phishingové kampane na svoju konštituenciu a informoval o zraniteľnostiach široko používaných IT produktov a systémov. Jednotka riešila aj vážnu phishingovú hrozbu, kedy boli škodlivé emaily rozposielané z účtov zamestnancov niekoľkých štátnych inštitúcií. Útočníci získali prístup ku týmto účtom v dôsledku úspešného phishingového útoku, pri ktorom obete vyplnili svoje prihlasovacie údaje do podvodného formulára.

CSIRT.SK riešil tiež kompromitácie webových sídiel a masívnu skenovaciu aktivitu.

Jednotka naďalej sledovala priebeh podvodnej telefonickej kampane, v ktorej sa zahraniční podvodníci vydávajú za technickú podporu Microsoftu, alebo inej všeobecne známej technologickej firmy a obetiam tvrdia, že ich zariadenia majú zraniteľnosť, alebo boli napadnuté hackermi.

Jednotka CSIRT.SK v decembri v rámci svojej proaktívnej činnosti testovala na zraniteľnosti niekoľko webových sídiel organizácií štátnej a verejnej správy, na základe požiadaviek. Informovala tiež o úniku útočných nástrojov spoločnosti FireEye v rámci útoku na platformu SolarWinds Orion. Odporučila bezodkladnú implementáciu protiopatrení vypracovaných spoločnosťou FireEye. CSIRT.SK dokončil testovanie bezpečnosti a analýzu zraniteľností v informačných systémoch zdravotníckych zariadení SR dostupných z internetu.

Štatistický prehľad incidentov riešených vládnou jednotkou CSIRT v roku 2020 môžete nájsť na našom webe.

Významné útoky vo svete

Výrobca lietadiel Embraer utrpel útok ransomvérom

Brazílska spoločnosť Embraer sa stala obeťou útoku ransomvérom. Po spoločnosti Boeing a Airbus sa jedná o tretieho najväčšieho výrobcu lietadiel na svete. Súbory tejto spoločnosti boli zdieľané na serveri na darkwebe spravovanom skupinou RansomExx (Defray777). Údaje zahŕňali vzorky informácií o zamestnancoch, obchodných zmlúv, fotografie leteckých simulácií a zdrojový kód. Spoločnosť uviedla, že útočníci mali prístup iba do jedného prostredia, a že incident mal iba dočasný dopad na niektoré z jeho operácií.

Na darkwebe sa predáva viac ako 250 tisíc databáz ukradnutých zo serverov MySQL

Útočníci na darkwebe predávajú 250 tisíc databáz ukradnutých z 83 tisíc kompromitovaných serverov MySQL. Uniknuté dáta majú veľkosť 7TB. Útočník vytvoril aukčný web, kde tieto databázy predáva. Veľkosť databáz sa pohybuje od 20B do niekoľkých GB a cena je 0.03 Bitcoinu. Za útokom stojí ransomvér PLEASE_READ_ME. Prvýkrát boli útoky týmto ransomvérom spozorované už v januári 2020, pričom druhá fáza sa začala v októbri. Operátori ransomvéru sa snažia zefektívniť svoje útoky dvojitým vydieraním.

Spoločnosť TransLink sa stala obeťou ransomvéru Egregor

Ransomvér Egregor narušil chod služieb a platobných systémov spoločnosti TransLink v kanadskom Vancouveri. K útoku došlo 1. decembra 2020, pričom obyvatelia neboli schopní používať svoje karty Compass slúžiace na cestovanie metrom. Narušená bola tiež funkčnosť kioskov a teda nebolo možné zakúpiť si lístky na metro. Predstavitelia spoločnosti TransLink spočiatku tento problém označili za technický; že išlo o

útok ransomvérom priznali až po dvoch dňoch. Funkčnosť kioskov a pokladní už spoločnosť obnovila.

Ransomvér DoppelPaymer odcudzil súbory spoločnosti Foxconn

Spoločnosť Foxconn, ktorá sa zaoberá výrobou elektroniky, utrpela útok ransomvérom. Útočníci pred šifrovaním zariadení ukradli súbory. Na webe ransomvéru DoppelPaymer boli zverejnené súbory patriace tejto spoločnosti. Uniknuté údaje zahŕňajú všeobecné obchodné dokumenty a správy, neobsahujú žiadne finančné informácie ani osobné údaje zamestnancov. Od útoku bola webová stránka zariadenia Foxconn CTBG MX nefunkčná. Útočníci požadujú výkupné vo výške 34 miliónov dolárov. Zašifrovali asi 1200 serverov, ukradli 100GB nezašifrovaných súborov a vymazali zálohy o veľkosti približne 20-30GB.

V rámci sociálnych sietí sa vyskytuje malvér známy ako skript Magecart

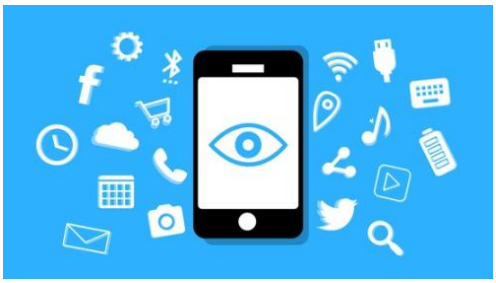
Útočníci vytvorili nový typ webového malvéru, ktorý sa ukrýva v obrázkoch tlačidiel určených na zdieľanie na sociálnych sieťach, používaných v internetových obchodoch. Cieľom tohto malvéru je ukradnúť informácie o kreditných kartách zadávané do platobných brán v internetových formulároch. Malvér je modifikáciou známeho skriptu Magecart a bol spozorovaný už v júni a septembri roku 2020. Tento konkrétny skript využíva techniku známu ako steganografia (skrytie informácií v inom formáte). Zaujímavosťou posledných útokov je, že škodlivý kód nebol ukrytý vo formátoch PNG alebo JPG, ale v SVG.

Spoločnosť Forward Air sa stala obeťou ransomvéru Hades

Prepravná a nákladná logistická spoločnosť Forward Air utrpela útok ransomvérom Hades. Spoločnosť bola donútená vypnúť svoje systémy, aby zabránila šíreniu ransomvéru. Útok viedol k prerušeniu činnosti, pretože dokumenty potrebné na prepustenie tovaru z colnice

boli uložené v systémoch, ktoré museli byť vypnuté. Nie je známe, koľko peňazí útočníci vyžadujú na obnovenie súborov a vzorka ransomvéru sa nenašla.

Nový malvér Goontact zasiahol zariadenia s operačným systémom Android aj iOS



Nový malvér s názvom Goontact existuje vo verziách pre Android aj iOS. Má schopnosť zhromažďovať z infikovaných zariadení údaje ako telefónne identifikátory, kontakty, SMS správy, fotografie a informácie o polohe. Tento malvér sa distribuuje prostredníctvom webov tretích strán propagujúcich bezplatné aplikácie okamžitých správ určené na poskytovanie eskortných služieb. Malvér sa zatiaľ nedostal do oficiálnych obchodov spoločností Apple a Google. Údaje zhromaždené z týchto aplikácií sa odosielajú späť na servery pod kontrolou operátorov Goontact. Na základe jazyka používaného pre administračné panely je pravdepodobné, že operáciu Goontact riadia čínsky hovoriaci útočníci.

15 rozšírení prehliadača Chrome a 13 rozšírení prehliadača Edge obsahuje škodlivý kód

Viac ako 3 milióny používateľov si nainštalovalo do svojich zariadení 15 rozšírení prehliadača Chrome a 13 rozšírení prehliadača Edge, ktoré obsahujú škodlivý kód. Týchto 28 rozšírení obsahovalo kód, ktorý mohol vykonávať operácie ako presmerovanie používateľov na phishingové stránky, zhromažďovanie osobných údajov, zber histórie prehliadania a podobne. Podľa výskumníkov spoločnosti Avast bol hlavným cieľom tejto kampane finančný zisk. Nie je známe, či boli rozšírenia už vytvorené so škodlivým kódom, alebo bol tento kód pridaný neskôr. Väčšina z týchto rozšírení sa vydávala za doplnky, ktoré mali používateľom pomôcť stiahnuť rôzny obsah zo sociálnych sietí ako Instagram, Facebook alebo Spotify.

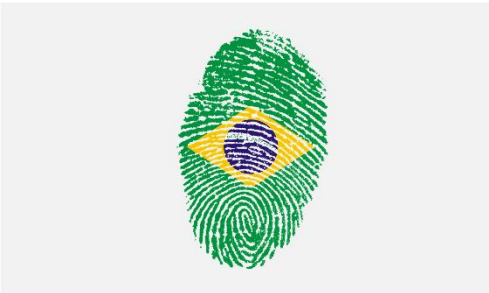
Útok na dodávateľa energií People's Energy ovplyvnil 270 tisíc zákazníkov

Britský dodávateľ energií People's Energy utrpel útok, ktorý zasiahol niektoré z osobných údajov súčasných aj bývalých zákazníkov. V súčasnosti má táto spoločnosť 270 tisíc zákazníkov, pričom zasiahnutí boli všetci z nich. Spoločnosť uviedla, že neoprávnená tretia strana získala prístup k jednému zo systémov na ukladanie údajov o členoch. Uniknuté údaje zahŕňajú mená, telefónne čísla, adresu bydliska, emailové adresy, dátumy narodenia a podobne. Incident nemal vplyv na heslá používateľských účtov.

Útočník zverejnil údaje o používateľoch peňaženky Ledger na kryptomeny

Útočník zadarmo na hackerskom fóre zverejnil ukradnuté e-mailové a poštové adresy používateľov peňaženky Ledger na kryptomeny. V júni 2020 Ledger utrpel únik údajov kvôli zraniteľnosti na webovej stránke, ktorá umožnila tretím stranám prístup ku kontaktným údajom zákazníkov. V decembri toho istého roku útočník zdieľal archív obsahujúci dva súbory „All Emails (Subscription).txt" a „Ledger Orders (Buyers) only.txt", ktoré obsahovali odcudzené údaje. Prvý súbor obsahuje emailové adresy viac ako 1 milióna ľudí, ktorí sa prihlásili na odber bulletinu Ledger. Druhý súbor obsahuje mená, poštové adresy a telefónne čísla viac ako 200 tisíc ľudí. Zverejnenie týchto údajov na fóre predstavuje značné riziko, pretože je možné ich zneužiť napríklad pri phishingových útokoch.

Unikli údaje o 243 miliónoch obyvateľov Brazílie



Osobné údaje o viac ako 243 miliónoch obyvateľov Brazílie boli zverejnené online. Vývojári webu nechali heslo pre kľúčovú vládnu databázu v zdrojovom kóde oficiálneho webu brazílskeho ministerstva zdravotníctva. Zdrojový kód obsahoval používateľské meno a heslo uložené v Base64. Prihlasovacie údaje umožňovali prístup k oficiálnej databáze brazílskeho ministerstva zdravotníctva, ktorá uchováva údaje o obyvateľoch Brazílie, ktorí sa prihlásili do systému

zdravotnej starostlivosti. Databáza obsahuje celé mená, adresu, telefónne čísla a lekárske informácie. Prihlasovacie údaje boli z webovej stránky odstránené. Nie je známe, či údaje o brazílskych občanoch boli ukradnuté.

Spoločnosť E-land sa stala obeťou útoku ransomvérom CLOP

Spoločnosť E-Land Retail bola nútená po útoku ransomvérom CLOP vyradiť z prevádzky 23 pobočiek NC Department a New Core. Informácie a údaje o zákazníkoch neboli odcudzené vzhľadom k tomu, že sú uložené a šifrované na samostatnom serveri. Skupina, ktorá stojí za týmto ransomvérom tvrdí, že v priebehu jedného roka ukradla juhokórejskému maloobchodníkovi E-Land 2 milióny kreditných kariet v rámci kampane, ktorá vyvrcholila útokom na spoločnosť v novembri roku 2020. Skupina do organizácie prenikla už skôr a dáta kradla pomocou malvéru typu point-of-sale (POS). Spoločnosť E-Land uviedla, že útok ransomvérom na server ústredia spoločnosti vynútil zatvorenie niektorých obchodov, ale spôsobil škody aj na sieti a systémoch.

- **Microsoft uviedol, že útočníci podporovaní vietnamskou vládou nasadzujú malvér na ťažbu kryptomien za účelom špionáže.**
- **Aplikácia GO SMS Pro stále vystavuje súkromné správy miliónov užívateľov.**
- **Bol odhalený nový phishingový útok s cieľom ukradnúť prihlasovacie údaje pre videokonferenčnú službu Zoom.**
- **Zálohy banky na Kajmanských ostrovoch ostali nezabezpečené a unikali z nich citlivé údaje.**
- **Botnet Xanthe sa zameral na nesprávne nakonfigurované Docker API.**
- **Malvér nazývaný Crutch využíva ako zadné vrátka Dropbox na exfiltráciu citlivých dokumentov.**
- **Aplikácie pre Android s viac ako 250 miliónmi stiahnutí sú stále náchylné na zraniteľnosť v knižnici Google, ktorá bola opravená v auguste 2020.**
- **Nový modul malvéru TrickBot infikuje UEFI firmvér.**
- **Skupina DeathStalker využíva zadné vrátka s názvom PowerPepper na špionáž cieľových systémov.**
- **Americký obchodný dom Kmart utrpel útok ransomvérom.**
- **Spoločnosť Randstad v Holandsku potvrdila útok ransomvérom Egregor.**
- **Výrobca vrtuľníkov Kopter sa stal obeťou ransomvéru.**
- **Spoločnosť Jonhson & Johnson sa stala obeťou severokórejskej skupiny útočníkov.**
- **Spoločnosť Netgain bola po útoku ransomvérom nútená vypnúť niektoré zo svojich dátových centier.**
- **Nová verzia malvéru Qbot automaticky odstráni všetky stopy po reštartovaní alebo po prebudení systému z režimu spánku.**
- **Bola zverejnená funkčná ukážka kódu ako obísť autentifikačný protokol Kerberos.**

TLP: White

- **Útočníci môžu zneužiť niektoré verzie nástroja WinZip na podsunutie malvéru alebo podvodného obsahu.**
- **Čínska APT skupina je podozrivá z útokov na mongolské vládne agentúry.**
- **Facebook narušil činnosť dvoch skupín útočníkov – jednej z Vietnamu a druhej z Bangladéša.**
- **Malvér Adrozek extrahuje údaje zo zariadení a kradne prihlasovacie údaje.**
- **Spoločnosť Intel Habana Labs bola zasiahnutá ransomvérom Pay2Key.**
- **Botnet PGMiner zneužíva PostgreSQL na distribúciu.**
- **Nórska spoločnosť Hurtigruten bola zasiahnutá kybernetickým útokom.**
- **Nový trójsky kôň v operačnom systéme Windows sa zameriava na procesy Outlooku a prihlasovacie údaje v prehliadačoch.**
- **Boli objavené nové škodlivé balíčky RubyGems, ktoré sa používajú pri krádeži kryptomien.**
- **Útok ransomvérom na počítačové systémy mesta Independence spôsobil, že niektorí obyvatelia neboli schopní platiť účty.**
- **Útočník otvoril 2 732 PickPoint skriniek na balíky po celej Moskve.**
- **Orgány činné v trestnom konaní sa zmocnili jednej z domén webovej stránky Joker's Stash.**
- **Emotet sa po dvojmesačnej prestávke vracia a zasahuje denne 100-tisíc cieľov.**
- **Skupina Lazarus podniká útoky proti dvom subjektom zapojeným do výskumu ohľadom COVID-19.**
- **Ruská burza kryptomeny Livecoin bola napadnutá útočníkmi a stratila kontrolu nad niektorými zo svojich serverov.**
- **Spoločnosť Whirlpool bola zasiahnutá ransomvérom Nefilim.**

- **Nový červ premieňa Windows a Linux servery na ťažiarov kryptomeny Monero.**
- **Emotet zasiahol litovské Národné centrum verejného zdravia.**
- **Spoločnosť T-Mobile potvrdila únik údajov, ktorý odhaľuje údaje ako telefónne čísla a záznamy hovorov.**
- **FBI vydalo varovanie pred útokmi ransomvérom DoppelPaymer.**

Závažné zraniteľnosti bežných softvérových produktov

V NAS zariadeniach od spoločnosti QNAP bolo opravených 6 závažných zraniteľností

Štyri zo závažných zraniteľností sa vyskytujú vo vstavanej aplikácii QTS, alebo QuTS hero v NAS zariadeniach. Ďalšia súvisí s aplikáciou Photo Station a posledná s Multimedia Console. Všetky tieto chyby sú typu XSS a umožňujú útočníkom injektovať škodlivý kód do NAS zariadení, čo môže viesť až ku prevzatiu kontroly nad zraniteľným zariadením.

V softvéri na správu medicínskych zobrazovacích prístrojov spoločnosti GE Healthcare sa vyskytujú 2 kritické zraniteľnosti

Kritické zraniteľnosti súvisia s predvolenými prihlasovacími údajmi do softvéru, ktorý je určený na správu medicínskych zobrazovacích prístrojov. Údaje sú voľne dostupné na internete a môžu byť zneužité na vykonávanie ľubovoľného kódu alebo na spôsobenie nedostupnosti zariadenia. Zneužitím týchto zraniteľností môžu byť taktiež pozmenené citlivé údaje.

V aplikácii Cisco Jabber bolo nájdených a opravených niekoľko závažných zraniteľností

Nájdené zraniteľnosti sa týkajú aplikácie Cisco Jabber. Tri z nich sú známe už dlhšie, avšak septembrovou aktualizáciou sa ich nepodarilo úplne odstrániť. Kritická zraniteľnosť umožňuje injektovať ľubovoľný skript a následne vzdialene vykonávať ľubovoľný kód. Závažné zraniteľnosti môžu tiež viesť k vzdialenému vykonávaniu kódu, prípadne k úniku citlivých informácií. Nájdené a opravené boli aj stredne závažné zraniteľnosti. Voči týmto chybám je vo všeobecnosti zraniteľný Cisco Jabber pre Windows, MacOS, ale aj pre Android a iOS.

Mesačník zraniteľností December 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
    - V NAS zariadeniach od spoločnosti QNAP bolo opravených 6 závažných zraniteľností
    - V softvéri na správu medicínskych zobrazovacích prístrojov spoločnosti GE Healthcare sa vyskytujú 2 kritické zraniteľnosti VMware - kritické zraniteľnosti v ESXi, Workstation, Fusion a NSX-T
    - V aplikácii Cisco Jabber bolo nájdených a opravených niekoľko závažných zraniteľností

https://www.csirt.gov.sk/aktualne-7d7.html?id=233