MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

CSIRT.SK

Mesačná správa CSIRT.SK

August 2020

Vypracoval: CSIRT.SK

TLP: White

Online banking predstavuje pohodlný spôsob na vedenie účtov, vybavenie platieb a transakcií z pohodlia domova pre mnohých z nás. Okrem uľahčenia rôznych povinností však so sebou prináša aj bezpečnostné riziko odcudzenia osobných či platobných údajov. Na tento účel útočníkom slúži trójsky kôň, skrátene trojan, ktorý tváriac sa ako bežný softvér, vykonáva v systéme používateľa škodlivú činnosť na pozadí.

Jedným z najznámejších malvérov patriacich medzi trojanov je Emotet. Tento malvér, hoci zo začiatku fungoval ako bankový trojan, postupom času zmenil svoju činnosť. Prvýkrát bol Emotet identifikovaný už v roku 2014 organizáciou FortiGuard Labs. Jeho neskoršie verzie fungovali ako tzv. loader-y, čiže malvéry ktoré sa dostanú do systému, získajú k nemu prístup a následne sťahujú dodatočné súbory do počítača obete – napríklad ďalšie škodlivé súbory. V súčasnosti Emotet funguje hlavne ako dropper, čo znamená že do systému sťahuje ďalší malvér (napríklad bankového trojana či ransomvér) zo škodlivého servera.

Malvér Emotet sa neskôr vo väčšom množstve prípadov objavil v rokoch 2018 a 2019. V júli tohto roku sa znovu začal objavovať v emailových schránkach. Primárne sa šíri pomocou spamových emailových správ. Stiahnutie malvéru môže zapríčiniť škodlivý skript, URL adresa alebo dokument v prílohe obsahujúci škodlivé makro. Posledný z týchto spôsobov je najčastejšou cestou, ktorú využívajú útočníci na šírenie Emotetu v posledných mesiacoch. Na to aby používateľ bol ochotný kliknúť na škodlivú prílohu, používajú útočníci lákavé mená pre dokumenty v emailovej správe – prílohy sa tvária ako faktúry, objednávky, či očakávané balíky od známych doručovacích firiem. Po otvorení prílohy sa na pozadí spustí makro a malvér spustí svoju činnosť.

Škodlivé makro v systéme používateľa spúšťa PowerShell kód. Tento kód je obfuskovaný a je tiež zakódovaný, zvyčajne vo formáte Base64. V programe PowerShell následne prebieha hlavná funkcia dropperu – stiahnutie dodatočných škodlivých súborov do infikovaného počítača. Tie sa ukladajú do priečinkov s názvami pozostávajúcimi z náhodných reťazcov. Súbory sú sťahované z IP adries serverov, na ktoré ich pridávajú pravdepodobne samotní útočníci. Ich účel sa môže líšiť. Podľa známych prípadov a analýz Emotet sťahuje rôzne súbory od bankových trojanov a ďalších dropperov, až po ransomvér.

Emotet sa nesústredí na konkrétnych používateľov, ale cieľové emailové adresy získava pravdepodobne aktívnym vyhľadávaním emailových zoznamov na internete. Malvér prešiel značným vývojom od jeho prvej vzorky a v nových verziách podvodných emailov už využíva aj personalizované správy obsahujúce napríklad mená či názvy spoločností. Stáva sa preto o to väčšou hrozbou. Podvodné emailové správy obsahujú texty v rôznych jazykoch, preto jediným spôsobom ako ho rozpoznať je analýza prílohy, ktorá zabezpečuje jeho stiahnutie do hostiteľského systému.

Riešené incidenty na Slovensku a z našej činnosti

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

Jednotka riešila vážnejší incident v rámci jednej organizácie zo svojej konštituencie, s podozrením na aktívnu hrozbu zvnútra v podobe zamestnanca.

V rámci svojej proaktívnej činnosti jednotka CSIRT.SK rozposlala svojej konštituencii varovanie pred kampaňou šíriacou ransomvér pomocou droppera Emotet. Ku nej poskytla aktuálne indikátory kompromitácie (IoC) v podobe IP adries, domén a hašov škodlivých súborov. CSIRT.SK varoval aj pred kampaňou severokórejskej APT skupiny Lazarus, nazvanou Dream Job. Skupina predstierala identitu amerických spoločností z leteckého a obranného sektoru - Boeing, McDonnell Douglas, BAE a podobne. Rozposielala v ich mene lákavé pracovné ponuky, ktorých prílohou boli škodlivé súbory. CSIRT.SK v rámci varovania informoval aj o indikátoroch kompromitácie spojených s touto hrozbou. Tiež informoval NBÚ o dokumente s uniknutými heslami, z ktorých niektoré patrili slovenským účtom.

Reprezentatívnu a edukačnú činnosť zastrešuje účasť jednotky na Letnej škole kyberkriminality v Danišovciach. Podujatia sa zúčastnilo viacero členov CSIRT.SK, pričom väčšina z nich aktívne – prednáškami, vedením cvičení a pomocou s organizačnými činnosťami.

Významné útoky vo svete

Výrobca fotoaparátov Canon bol zasiahnutý ransomvérom

Cloudové úložisko spoločnosti Canon s názvom image.canon určené na ukladanie fotografií a videí obnovilo prevádzku po takmer šiestich dňoch výpadku. Spoločnosť oznámila technické problémy a stratu niektorých fotografií a videí. Súčasne bola narušená dostupnosť mnohých webových stránok spoločnosti. Špecialisti z BleepingComputer získali údajnú požiadavku o výkupné, podľa ktorej uniklo 10TB dát. Pravdepodobne sa jednalo o útok ransomvéru Maze. Útočníci stojaci za týmto ransomvérom potvrdili útok na spoločnosť Canon, avšak vylúčili spôsobenie výpadku. O niekoľko dní operátori ransomvéru Maze zverejnili databázu o veľkosti 2.2GB ktorá obsahovala 5% z uniknutých dát. Spoločnosť Canon sa k situácii zatiaľ nevyjadrila.

Spoločnosti Intel uniklo 20 GB dát, vrátane dôverných dokumentov

Zbierka tajných dát spoločnosti Intel o veľkosti 20GB unikla na verejnú službu zdieľania súborov. Dáta obsahovali zdrojové kódy aj utajované informácie, vrátane duševného vlastníctva. Anonymný zdroj tvrdí, že našiel nezabezpečený server a zistil, že sa dokáže dostať k akémukoľvek priečinku ak pozná jeho meno. Z priečinka sa dostal do koreňového adresára a získal prístup ku všetkým dátam servera. Uverejnené dáta mali byť len časťou zo všetkých získaných dát. Podľa Intelu by dáta mali pochádzať z Intel Resource and Design centra. Zamestnanci tohto centra majú vysoké privilégia a prístup ku duševnému vlastníctvu spoločnosti.

Útočníci získali prístup do moderátorských kont Redditu

V koordinovanom útoku bolo odcudzené množstvo moderátorských kont Redditu. Odcudzené boli len tie, ktoré nemali aktivovanú 2-faktorovú autentifikáciu. Tie boli použité na zverejňovanie správ podporujúce amerického prezidenta Donalda Trumpa a mazanie kont nižších administrátorov. Útočníci sa priznali k útoku cez kompromitované konto na Twitteri. Tvrdili, že administrátori mali veľmi jednoduché heslá, takže bolo možné, že sa k nim dostali útokom hrubou silou. Administrátori Redditu dané kontá uzamkli, zvrátili

zmeny útočníkov a kontá vrátili pôvodným majiteľom.

Inštitútu SANS unikli dáta po úspešnom phishingovom útoku

SANS je jednou z najväčších organizácií pre vzdelávanie sa v oblasti informačnej bezpečnosti. Jeden z ich zamestnancov bol obeťou phishingovému útoku, ktorý umožnil útočníkovi získať prístup k jeho e-mailovému účtu. Pri kontrole konfigurácie zamestnanci zistili, že útočník nakonfiguroval pravidlo, ktoré preposiela všetky e-maily prijaté v tomto účte na neznámu externú e-mailovú adresu a nainštaloval škodlivý doplnok Office 365. Týmto spôsobom uniklo 513 emailov s približne 28 tisíc záznamami obsahujúcimi osobné informácie.

Výrobcovi alkoholických nápojov Brown-Forman uniklo 1TB údajov

Jeden z najväčších výrobcov alkoholických nápojov v USA - Brown-Forman bol cieľom útoku ransomvérom. Skupina útočníkov REvil oznámila, že sa dostala do siete spoločnosti a získala 1TB dát, ktoré mali obsahovať dôverné informácie o zamestnancoch, kontraktoch, obchodoch a financiách spoločnosti. Časť údajov zverejnili. Útok bol včas odhalený a zastavený skôr, ako došlo k šifrovaniu. Napriek tomu skupina REvil požadovala výkupné, keďže uniknuté údaje majú obsahovať dáta, ktoré by mohli byť užitočné pre konkurenciu. V prípade nezaplatenia výkupného ich chcú predať na aukcii. Brown-Forman však odmieta útočníkom zaplatiť.

Kanadskú vládu zasiahol kyberútok

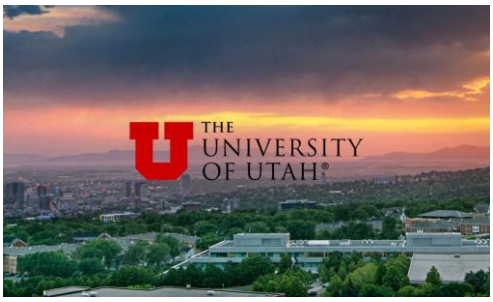
Kanadské vládne stránky boli cieľom koordinovaného útoku s cieľom kradnúť financie určené na zmiernenie finančnej krízy spôsobenej pandémiou. Viaceré stránky používajú single sign-on službu GCKey na prístup pre verejnosť. Využitím kombinácií mien a hesiel uniknutých z iných zdrojov, získali útočníci prístup k 9041 kontám. Rovnaký útok sa nedávno odohral na Canadian Revenue Agency (CRA). Do CRA je možné prihlásiť sa priamo cez CRA účet, alebo cez GCKey. Jednou z využívaných transakcií je požiadanie o finančný príspevok až do výšky 2000 kanadských dolárov. Práve ten bol cieľom útočníkov. Cez kontá obetí požiadali o príspevok, ktorý dali poslať na svoje účty. Po odhalení útoku boli kompromitované kontá blokované a používatelia dostali inštrukcie na získanie nového GCKey kľúča.

TLP: White

Prevádzkovateľ výletných lodí Carnival bol zasiahnutý ransomvérom

Carnival Corporation, najväčší svetový prevádzkovateľ výletných lodí ohlásil, že ransomvér zašifroval systémy jednej z ich spoločností. Okrem toho predpokladajú, že boli odcudzené dáta spoločnosti. Carnival odmieta poskytnúť akékoľvek bližšie informácie, keďže incident je v štádiu vyšetrovania. Podľa bezpečnostnej spoločnosti Bad Packets mala spoločnosť Carnival zraniteľné zariadenia prístupné zo siete Internet. Carnival bol cieľom iného útoku už v marci 2020. V tom čase sa útočník dostal do mailových kont zamestnancov, následkom čoho unikli osobné údaje zákazníkov.

Univerzita v Utahu zaplatila výkupné vo výške 457 tisíc dolárov po útoku ransomvérom



Fakulta College of Social and Behavioral Science (CSBS) Univzsity of Utah bola zasiahnutá ransomvérom, ktorý zašifroval obsah serverov. Súčasne útočníci odcudzili dáta zo serverov fakulty. Tie obsahovali osobné informácie študentov a zamestnancov. Aby univerzita zabránila zverejneniu údajov, rozhodla sa zaplatiť výkupné. Na tento účel mala univerzita uzatvorené kyber poistenie. Tento typ poistenia pokrýva aj útoky ransomvérom a je možné použiť ho pri platbe výkupného. Univerzita zaplatila 457 tisíc dolárov, pričom celá suma bola pokrytá poistením. Útoky na univerzity nie sú výnimkou. V júni 2020 zaplatila The University of California San Francisco výkupné 1,14 milióna dolárov.

Spoločnosti Freepik uniklo 8,3 milióna záznamov

Freepik, poskytovateľ obrázkov, ilustrácií a grafických dizajnov, oznámil únik údajov. Útočníci získali pomocou útoku SQL injection 8,3 milióna záznamov, ktoré obsahovali prihlasovacie údaje používateľov. Pri tomto type útoku sa do používateľského vstupu zadá príkaz pre databázu, ktorý sa bez ošetrenia vykoná a vráti výsledky. 3.55 milióna používateľov malo uloženú len emailovú adresu, keďže používali externé prihlásenie. Ostatní používatelia mali uložený hash hesla so „soľou“ (reťazec ktorý sa pridá pred hashovaním aby bolo náročnejšie získať pôvodné heslo), ale 229 tisíc hesiel bolo hashovaných algoritmom MD5, ktorý je ľahké prelomiť. Freepik preto kontá týchto používateľov resetoval.

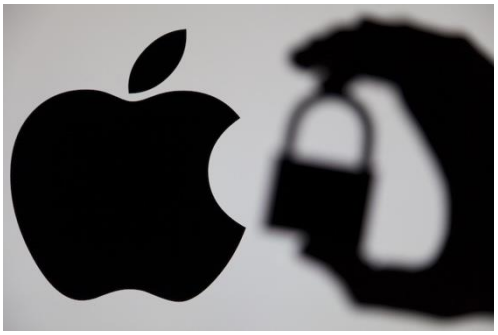
Útočníci získali dáta architektonickej spoločnosti

Obeťou Incidentu, ktorý vyšetrovala spoločnosť Bitdefender, bola veľká architektonická spoločnosť, ktorá pracuje s luxusnými nehnuteľnosťami a nechce byť menovaná. Útočníci využili vtedy neznámu zraniteľnosť grafického softvéru Autodesk 3ds Max, ktorá umožňovala spustenie kódu na zariadení obete. Škodlivý kód sa distribuoval vo forme MAXScript pluginu nazvaného PhysXPluginMfx. Ten dokázal šíriť škodlivý kód v sieti obete a využíval techniky na vyhnutie sa detekcii. Cieľom tohto malvéru bola špionáž. Malvér kontaktoval riadiace servery v Južnej Kórei, ktoré sú spojené s viacerými inými útokmi. Vzhľadom na zložitosť útoku spoločnosť Bitdefender predpokladá, že šlo o APT skupinu najatú na industriálnu špionáž.

Burza Nového Zélandu bola napadnutá DDoS útokom

New Zealand's stock exchange (NZX) bola po dobu štyroch dní napádaná distribuovaným útokom s cieľom narušiť jej dostupnosť (DDoS). Útoky prišli v čase, keď spoločnosti ohlasovali ročné finančné výsledky, ktoré boli poznačené krízou spôsobenou koronavírusom. To spôsobovalo veľkú volatilitu akcií, čo mohlo finančne motivovať útočníka. Podľa NZX útoky pochádzajú z oblasti mimo Nového Zélandu, ale kompetentní odmietli uviesť krajinu, keďže incident je ešte v procese vyšetrovania. CERT Nového Zélandu ešte v novembri 2019 varoval pred výhražnými emailmi, ktoré dostali mnohé finančné spoločnosti krajiny. V nich sa útočníci vyhrážali DDoS útokom v prípade, že nedostanú výkupné. Autori tvrdili, že patria k známej ruskej hackerskej skupine Fancy Bear. Neznámy zdroj tvrdil, že v tomto prípade ide o skupinu DDoS vydieračov, ktorá pri výhražných mailoch používa mená iných známych skupín. Táto skupina podľa zdroja zaútočila v rovnaký týždeň na finančné spoločnosti MoneyGram, YesBank India, Worldpay, PayPal, Braintree, a Venmo. Niektoré z nich tiež ohlásili incidenty spojené s nedostupnosťou ich služieb.

Autorom škodlivého Shlayer sa podarilo obísť kontrolu malvéru na zariadeniach Apple



Od februára 2020 platí, že všetok softvér zariadení Apple distribuovaný mimo App Store musí byť schválený spoločnosťou Apple, aby mohol byť spustený. Časťou schvaľovacieho procesu je kontrola prítomnosti malvéru. Malvér Shlayer sa neznámym spôsobom cez tento proces dostal. Po jeho nahlásení bol jeho certifikát zablokovaný, ale krátko potom boli objavené ďalšie schválené verzie malvéru, ktoré boli obsahom takmer identické. Tento malvér inštaluje mitmdump proxy, vďaka čomu môžu útočníci analyzovať a modifikovať šifrovanú prevádzku protokolu HTTPS. To môže byť zneužité na podvrhnutie reklám a škodlivých skriptov do navštevovaných stránok. Súčasne môžu útočníci získavať údaje aj zo šifrovaných stránok, ako je napríklad online banking.

- **Útočníci stojaci za ransomvérom Maze zverejnili desiatky gigabajtov interných údajov od spoločností LG a Xerox**
- **Aplikácia Zello potvrdila únik dát, ktoré obsahovali emailové adresy a hashované heslá používateľov**
- **Platforma 2gether určená na obchodovanie s kryptomenami bola obeťou útoku, pri ktorom bolo odcudzených 1,2 milióna eur v kryptomenách**
- **Havenly, webová stránka zameraná na interiérový dizajn, potvrdila, že došlo k úniku údajov po tom, čo útočník zdarma zverejnil databázu obsahujúcu 1,3 milióna záznamov**
- **Cestovná spoločnosť CWT bola napadnutá ransomvérom a následne zaplatila útočníkom výkupné 4,5 milióna dolárov**
- **Mesto v americkom Colorade bolo po útoku ransomvérom nútené zaplatiť výkupné 45 tisíc dolárov po tom, čo nedokázalo obnoviť potrebné súbory zo zálohy**
- **Skupina 295 rozšírení pre prehliadač Chrome sledovala výsledky vyhľadávania zo služieb Google a Bing**
- **Útočník zverejnil zoznam používateľských mien a hesiel spolu s IP adresami viac ako 900 serverov Pulse Secure VPN**
- **Nový druh útoku určený na zbieranie údajov o kreditných kartách využíva útoky pomocou homoglyfov**

TLP: White

- **FBI varuje pred iránskymi útočníkmi, ktorí využívajú zraniteľnosť v sieťových zariadeniach F5**
- **Systém na monitorovanie online testov ProctorU potvrdil únik údajov po tom, čo ich databáza bola zverejnená online**
- **Phishingový útok zameraný na používateľov softvéru cPanel využíval falošné bezpečnostné upozornenia, ktoré varovali pred kritickými zraniteľnosťami**
- **Skupina útočníkov s názvom RedCurl zameriavajúca sa na špehovanie podnikov je aktívna už tri roky**
- **FBI a NSA varujú pred novým malvérom určeným na linuxové systémy s názvom Drovorub, ktorý je využívaný ruskými štátnymi hackermi**
- **Nový malvér XCSSET zameraný na systémy s operačným systémom macOS sa šíri pomocou Xcode projektov a využíva dve zero-day zraniteľnosti**
- **APT skupina s názvom CactusPete vylepšuje svoje nástroje na ich využitie proti finančným a vojenským spoločnostiam v celej Európe**
- **Ransomvér s názvom DarkSide zasiahol severoamerického developera nehnuteľností**
- **Útočníci začali vykonávať cielené útoky pomocou ransomvéru s názvom DarkSide, ako výkupné požadujú milióny dolárov**
- **Skupina útočníkov Lazarus sa zameriava na spoločnosti pracujúce s kryptomenami prostredníctvom správ na sieti Linkedin**
- **Juhoafrická pobočka spoločnosti Experian oznámila únik údajov, ktorý má dopad na 24 miliónov zákazníkov**
- **Vláda USA varuje pred severokórejskými hackermi, ktorí znova útočia na banky po celom svete**
- **Útočníci zneužívajú zraniteľnosti v platforme WooCommerce pre Wordpress, ktorá bola inštalovaná viac ako 30 tisíc krát**
- **Útočník zverejnil databázy stránok zameraných na výmenu zbraní, pôsobiacich v Utahu**
- **Obchodný technologický gigant Konica Minolta bol zasiahnutý ransomvérom, ktorý ovplyvnil ich služby takmer na týždeň**

Závažné zraniteľnosti bežných softvérových produktov

Zraniteľnosť v softvéri Cisco ASA a FTD firewall umožňuje čítať súbory servera

Kvôli nedostatočnej validácii URL adresy z HTTP požiadaviek v produkte Cisco ASA a FTD firewall môže útočník vložiť do požiadavky cestu súborového systému servera. Vďaka tomu môže pristúpiť k dátam ktoré nie sú určené pre používateľov.

Kritická zraniteľnosť v komponentoch .NET, SharePoint a Visual Studio umožňuje deserializáciu akéhokoľvek kódu

Opravená kritická zraniteľnosť sa nachádza v .NET Framework a produktoch SharePoint a Visual Studio. Prejavuje sa tým, že komponenty .NET slúžiace na prácu s datasetmi neskontrolujú zdrojový markup spracovaného XML súboru. Vďaka tomu útočník môže .NET aplikácii poslať XML súbor obsahujúci kód ktorý aplikácia vykoná.

Zraniteľnosť zavádzača GRUB2 ohrozuje väčšinu Windows a Linux systémov

Spoločnosť Eclypsium objavila závažnú zraniteľnosť v zavádzači GRUB2, ktorá umožňuje vložiť do kódu zavádzača malvér, obísť mechanizmus Secure boot a získať perzistenciu aj v prípade reinštalácie operačného systému.

Kritická zraniteľnosť v aplikácii vBulletin umožňuje vzdialené vykonávanie kódu bez autentifikácie

Zraniteľnosť v aplikácii vBulletin je spôsobená nedostatočnou kontrolou používateľských vstupov a viaže sa na nedostatočnú záplatu staršej zraniteľnosti. Na zneužitie je potrebné poslať príkaz na renderovanie vlastnej šablóny s PHP konfiguračným kódom ktorý sa vykoná. Aplikácia vykoná príkaz aj bez autentifikácie.

TLP: White

Zraniteľnosť v aplikácii TeamViewer umožňuje útočníkovi pripojiť sa bez znalosti hesla

Nedostatočná kontrola vstupných parametrov URI schém aplikácie TeamViewer môže spôsobiť, že parametre sa vykonajú ako príkazy. Útočník tak môže podsunúť obeti vstup, ktorý spustí TeamViewer a vykoná požadovanú akciu. To je možné využiť na vytvorenie zdieľaného priečinka zo strany obete, vďaka čomu sa útočník nemusí autentifikovať.

Microsoft vydal núdzový update pre Windows 8.1 a Server 2012 R2 kvôli kritickým zraniteľnostiam

Obe kritické zraniteľnosti sa nachádzajú v službe Remote Access Service a umožňujú zvýšenie oprávnení vzdialenému útočníkovi v prípade, že už má do systému prístup so schopnosťou spúšťania programov.

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností, z toho kritické boli nasledujúce:
Multiple Vulnerabilities in Treck IP Stack Affecting Cisco Products CVE-2020-11896 - CVE-2020-11914: Sada predtým neznámych zraniteľností bola zverejnená 16. júna 2020. Zraniteľnosti sú súhrnne známe ako Ripple20. Zneužitie týchto chýb môže mať za následok vzdialené spustenie kódu, odmietnutie služby (DoS) alebo zverejnenie informácií, v závislosti od konkrétnej zraniteľnosti.
Cisco vWAAS Default Credentials Vulnerability CVE-2020-3446: Zraniteľnosť v Cisco Virtual Wide Area Application Services (vWAAS) s využitím Cisco Enterprise NFV Infrastructure Software (NFVIS) pre zariadenia Cisco ENCS 5400-W Series a CSP 5000-W Series by mohla umožniť neautentizovanému vzdialenému útočníkovi prihlásiť sa do NFVIS CLI postihnutého zariadenia pomocou účtov, ktoré majú predvolené, statické heslo.

Zraniteľnosti Intel

V produktoch Intel bolo opravených viacero rozličných závažných zraniteľností a 1 kritická zraniteľnosť:
Intel Server Boards, Server Systems and Compute Modules CVE-2020-8708: Nesprávne overenie totožnosti pre niektoré serverové systémy Intel a výpočtové moduly pred verziou 1.59 môže umožniť neautentizovanému používateľovi eskaláciu privilégií prostredníctvom nepriameho prístupu.

Mesačník zraniteľností August 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
   - Zraniteľnosť v softvéri Cisco ASA a FTD firewall umožňuje čítať súbory servera
   - Kritická zraniteľnosť v komponentoch .NET, SharePoint a Visual Studio umožňuje deserializáciu akéhokoľvek kódu
   - Zraniteľnosť zavádzača GRUB2 ohrozuje väčšinu Windows a Linux systémov
   - Kritická zraniteľnosť v aplikácii vBulletin umožňuje vzdialené vykonávanie kódu bez autentifikácie
   - Zraniteľnosť v aplikácii TeamViewer umožňuje útočníkovi pripojiť sa bez znalosti hesla
   - Microsoft vydal núdzový update pre Windows 8.1 a Server 2012 R2 kvôli kritickým zraniteľnostiam

https://www.csirt.gov.sk/aktualne-7d7.html?id=224