ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

CSIRT.SK

Mesačná správa CSIRT.SK

Júl 2019

Vypracoval: CSIRT.SK

TLP: White

V priebehu tohto mesiaca sa na viacerých IT portáloch objavila téma bezpečnosti pri používaní sociálnych sietí. Zaujímavý článok uverejnil server fastcompany.com. V ňom Stephanie "Snow" Carruthers, vedúca hackerka tímu IBM X-Force Red, ukázala, ako nevinné informácie, ktoré zdieľame, pomáhajú útočníkom dostať sa do systémov svojich obetí. V pozadí zdieľaných firemných fotiek je možné nájsť bezpečnostné prvky, ktoré spoločnosť používa, informácie na zapnutých počítačových obrazovkách, či niekedy dokonca heslá na žltých lepkách... Ak máte za chrbtom napríklad tabuľu so svojou obľúbenou tímovou aktivitou, môžete ľahko dostať phishingový e-mail s odkazom k jej aktuálnemu časovému plánu... ktorý vás však zavedie na stránku s malvérom. Fotky firemných preukazov a vstupových kartičiek uľahčia útočníkom výrobu dôveryhodne vyzerajúcich kópií a umožnia im fyzický prístup do spoločnosti. Dobrí sociálni inžinieri na verejne zdieľaných fotkách a videách z pracovného prostredia takmer vždy nájdu zaujímavý detail, ktorý im pomôže lepšie sa pripraviť na úspešný útok.

Okrem toho fotografie obsahujú metadáta, ktoré poskytujú (nielen) útočníkom cenný zdroj informácií. Na Facebook teda neputuje len samotný obrázok, ale aj informácie o jeho tvorcovi, mieste a čase, kde bol urobený. Preto si pred každým zdieľaním najprv premyslime, čo všetko o sebe verejne odhaľujeme a či sme s tým stotožnení. Dnešným fenoménom u rodičov je zdieľať fotografie zo života svojich ratolestí. Treba však zvoliť triezvu mieru, nakoľko tieto môžu pri nepremyslenom zdieľaní ohroziť bezpečnosť dieťaťa. Útočníci totiž môžu získať napríklad informácie o jeho pravidelných trasách, mieste školskej dochádzky, či záujmových krúžkov. Vaše dieťa môžete tiež ľahko diskreditovať zdieľaným obsahom v budúcnosti, nakoľko tým vytvárate jeho digitálnu stopu. Tej je veľmi obtiažne, ak nie priamo nemožné, sa zbaviť. To všetko môže viesť tiež ku zhoršeným rodinným vzťahom.

Na druhej strane deti potrebujú podporu a vedenie rodičov v online svete, vysvetľovanie hrozieb a možností ako sa pred nimi chrániť. Všímajte si, či vaše dieťa nie je obeťou kyberšikany, alebo či sa samo nespráva na sociálnych sieťach agresívne.

30. jún bol dňom sociálnych médií. Ľuďom mal priniesť do povedomia benefity, ktoré nám sociálne médiá poskytujú, no zároveň hrozby, ktoré prinášajú naše zbrklé rozhodnutia pri ich používaní. Pri tejto príležitosti spoločnosť Sophos prispela piatimi radami, ako na to:

1. Používajte silné heslo, aby útočníci nemohli získavať informácie o vás, ani zneužiť váš účet na útoky na vašich priateľov, rozposielanie spamu, či ilegálny predaj. Používajte manažér hesiel.
2. Používajte dvojfaktorovú autentifikáciu.
3. Pred zdieľaním videí, fotografií a informácií všeobecne si premyslite, či tieto chcete skutočne zdieľať s celým svetom. Chcete zverejniť váš dátum narodenia, ŠPZ vášho auta, či číslo vášho domu? Metadáta fotografií? Miesto, kde sa práve nachádzate? Či radostný tweet, že ste práve dorazili do vašej dovolenkovej destinácie, a teda že vaša domácnosť ostane nasledujúci týždeň bez dozoru?
4. Skontrolujte si bezpečnostné nastavenia svojich účtov. Kontrolujte ich pravidelne, pretože sa zvyknú meniť. Odporúča sa použiť notebook, pretože na telefóne môžu byť tieto menu menej prehľadné.

5. Ak je to možné, nezdieľajte svoju geolokáciu. Vypnite ju na svojich zariadeniach. Okrem prípadov, keď sa chystáte sami do hôr, alebo ste v neznámom meste :).

Ako je to teda s naším bezpečnostným povedomím? Štúdia spoločnosti Palo Alto Networks na 1300 Američanoch ukázala napríklad, že aj keď 2/3 z respondentov verí, že vykonávajú všetky potrebné kroky pre svoju bezpečnosť, len niečo málo vyše štvrtiny pri prijatí e-mailu od neznámeho odosielateľa v skutočnosti kontroluje jeho identitu. Podobne len štvrtina respondentov spustí antivírový sken svojho zariadenia, keď kliknú na škodlivý odkaz. Až 28% respondentov priznalo, že v práci nikdy nemali tréning IT bezpečnosti.

Okrem týchto a a vyššie uvedených odporúčaní pravidelne aktualizujte svoje aplikácie (nielen tie pre prístup na sociálne médiá). Inak umožníte útočníkom zneužiť už opravené závažné zraniteľnosti, aby si otvorili dvere dokorán k vášmu osobnému účtu so všetkým obsahom a funkciami, nad ktorými by ste mali mať moc len vy.

Riešené incidenty na Slovensku a z našej činnosti

CSIRT.SK v mesiaci júl riešil zväčša štandardné incidenty, najmä phishingové kampane na svoju konštituenciu. Tento mesiac sa tiež vyskytlo väčšie množstvo e-mailových kampaní šíriacich malvér, ako zvyčajne. Okrem toho CSIRT.SK riešil dva ransomvérové útoky. Ďalej CSIRT.SK prijal a overil hlásenie zraniteľnosti jednej aplikácie.

V rámci proaktívnej činnosti varoval CSIRT.SK svoju konštituenciu pred kritickou zraniteľnosťou operačných systémov Android 7.-9. verzie.

CSIRT.SK vykonal niekoľko vyžiadaných externých penetračných testov inštitúcií vo svojej konštituencii.

V rámci aktivít zameraných na zvyšovanie odbornej a vedomostnej úrovne tímu sa členovia CSIRT.SK zúčastnili na niekoľkých vzdelávacích a certifikačných podujatiach.

Významné útoky vo svete

1325 aplikácií pre Android zbiera používateľské dáta bez súhlasu

Bezpečnostní výskumníci z kalifornského International Computer Science Institute odhalili 1325 aplikácií pre Android, ktoré zbierajú používateľské dáta aj po zamietnutí používateľom. Aj bez povolenia dokážu získavať identifikačné údaje o telefóne (napríklad IMEI) a geolokačné infromácie. Využívajú na to rôzne špeciálne techniky, akými je exfiltrovanie metadát z fotografií, alebo informácií o wifi pripojeniach.

Grécky správca domény prvého rádu ICS-Forth napadnutý

Grécky správca domény prvého rádu ICS-Forth utrpel prienik do svojich systémov. Skupina Sea Turtle útočila na DNS providera, kde zmenila DNS záznamy spoločnosti. Tak mohla pokračovať útokom typu man-in-the-middle, presmerovať legitímnu komunikáciu a získať prihlasovacie údaje. Takéto útoky sa veľmi ťažko odhaľujú, nakoľko spoločnosti nezvyknú monitorovať zmeny v DNS nastaveniach.

MageCart skript v kóde vyše 17 000 webstránok

Útočníci z jednej z MageCart skupín injektovali škodlivým kódom na čítanie platobných kariet vyše 17 000 webstránok, vrátane mnohých z prvých 2000 pozícií rebríčka Alexa. Využili nesprávne nakonfigurované Amazon S3 úložiská, ktoré dovoľovali prístup k uloženým súborom a plošne injektovali svoj obfuskovaný škodlivý kód do JavaScript súborov.

Krádež osobných údajov vyše 70% Bulharov z Národnej príjmovej agentúry

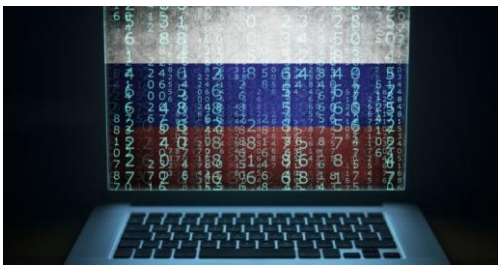
НАЦИОНАЛНА АГЕНЦИЯ
ЗА ПРИХОДИТЕ

Únik údajov z bulharskej Národnej príjmovej agentúry zasiahol väčšinu obyvateľov tejto krajiny. Zo 7 miliónovej populácie útočník ukradol citlivé osobné údaje až 5 miliónom Bulharov, vrátane mien, adries trvalého pobytu, identifikačných čísel a finančných ziskoch. Niektoré údaje sú staršieho dáta, od roku 2007.

TLP: White

Útočník odcudzil 110 databáz a odkazy na polovicu poslal lokálnym médiám. Tieto asi o týždeň zverejnil predávajúci so pseudonymom Instakilla na hackerských fórach.

Únik tajných projektov ruskej tajnej služby FSB



Útočníci sa nabúrali do Active Directory servera SyTech, zmluvného partnera ruskej tajnej služby FSB, a získali prístup do celej internej siete spoločnosti. Získali informácie o tajných kyber-špionážnych projektoch, na ktorých kontraktor pracoval. Unikli tak dáta o projektoch deanonymizácie prevádzky siete Tor, mapovania topológie ruského segmentu internetu, zberu dát používateľov sociálnych sietí, či monitoringu e-mailovej komunikácie ruských spoločností. Útočníci získali 7,5 TB dát, ktoré posunuli svojim kolegom z inej skupiny, no tiež médiám a na internet.

Spoločnosť Huawei tajne zbierala v Českej republike osobné údaje

Spoločnosť Huawei tajne zbierala v Českej republike osobné údaje zákazníkov a obchodných partnerov, priznali dvaja anonymní bývalí manažéri spoločnosti pre Český rozhlas. Ukladala ich na systém oddelený od komerčnej časti, prístupný z Číny. Informácie okrem iného obsahovali počet detí, záľuby a finančnú situáciu subjektov. Spoločnosť Huawei sa vyjadrila, že konala v súlade s nariadením GDPR.

Ransomvér zanechal časť obyvateľov juhoafrického Johannesburgu bez elektriny

Mestom Johannesburg vlastnená spoločnosť distribuujúca a vykupujúca elektrickú energiu utrpela ransomvérový útok. Spoločnosť City Power stratila schopnosť predávať a kupovať elektrickú energiu, a tiež rýchlo reagovať na výpadky prúdu. Zašifrovaná bola databáza spoločnosti, interná sieť, webové aplikácie a oficiálna webstránka. Útok zanechal časť obyvateľov najväčšieho mesta Juhoafrickej republiky bez elektrickej energie.

Ransomvér zablokoval prístup do policajnej databázy z policajných áut

Oddelenie verejnej bezpečnosti amerického štátu Georgia utrpelo ransomvérový útok. Zasiahnutý bol backend organizácie, čo spôsobilo prerušenie konektivity laptopov inštalovaných v policajných autách a stratu prístupu jednotiek ku dôležitým informáciám. Podľa všetkého sa infekcia prvýkrát objavila na služobnom notebooku, odkiaľ sa rýchlo rozšírila ďalej. Oddelenie vyplo všetky svoje systémy, aby zabránilo ďalšiemu šíreniu malvéru. Policajné zložky však dokázali operovať naďalej, pričom na získavanie potrebných informácií využívali vysielačky a služobné telefóny.

Osobné dáta 106 miliónov občanov USA a Kanady unikli po prieniku do systémov spoločnosti Capital One

Osobné dáta 100 miliónov občanov USA a 6 miliónov občanov Kanady žiadajúcich, alebo vlastniacich kreditnú kartu spoločnosti Capital One, unikli po prieniku do jej systémov. Únik obsahoval údaje o transakciách, hodnotenia kreditu, históriu platieb, zostatky na účtoch a v niektorých prípadoch tiež pridružené bankové účty a čísla sociálneho poistenia. Na prienik spoločnosť prišla pri vnútornom vyšetrovaní po tom, ako etický hacker nahlásil zraniteľnosť v jej systéme. Podozrivého útočníka zatkla FBI.

Okres Cabarrus v Severnej Karolíne prišiel o 1,7 milióna USD po úspešnom BEC podvode

Okres Cabarrus v Severnej Karolíne poslal 2,5 milióna USD na účet podvodníkov po úspešnom BEC podvode. Peniaze mali putovať staviteľskej firme, ktorá pre okres stavala novú strednú školu. Útočníci predstierajúci totožnosť staviteľskej spoločnosti poslali predstaviteľom okresu legitímne vyzerajúci e-mail so žiadosťou o zmenu bankového účtu, na ktorý mali peniaze vyplatiť. Podvod bol odhalený až tri týždne po vykonaní platby. Bankám sa podarilo získať naspäť len 776 000 USD. Okres musel zvyšok vyplatiť zo svojich rezerv.

- **Spoločnosť Online Buddies dostala pokutu za nezabezpečenie databázy súkromných a nahých fotiek členov svojej zoznamky Jack'd rok po upozornení.**

TLP: White

- **Útočníci kradnú prihlasovacie údaje do Instagramu pomocou premysleného phishingu sľubujúceho obetiam znak „verified“.**

- **Útok na kalifornského giganta PCM poskytujúceho cloudové služby zasiahol korporátnych klientov spoločnosti.**

- **Spoločnosť Orvibo vyvíjajúca smart home manažovaciu platformu mala nezabezpečený server Elasticsearch databázou. Dve miliardy záznamov citlivých zákazníckych dát ponechali nezabezpečené aj po upozornení.**

- **Firma Medtronic vymieňa pacientom inzulínové pumpy so závažnou zraniteľnosťou, ktorá sa nedá opraviť aktualizáciou.**

- **Ransomvérový útok na servery administratívnej kancelárie súdov amerického štátu Georgia.**

- **Policajné kamerové záznamy (nielen) polície Miami unikli z nezabezpečených úložísk a útočníci ich predávajú na darkwebe.**

- **Útočníci zneužili zraniteľnosť v aplikácii siete 7-Eleven a ukradli ich japonským zákazníkom pol milióna USD. Spoločnosť sľúbila obetiam kompenzáciu.**

- **Spear-phishingový útok na zamestnancov chorvátskej vlády šíril nový malvér.**

- **Nová MageCart kampaň - prienik do 962 internetových obchodov a inštalácia skriptu MageCart.**

- **Najväčší britský dodávateľ pre policajné forenzné laboratóriá Eurofins Scientific utrpel útok ransomvérom. Zaplatil výkupné.**

- **BEC útok (Business Email Compromise) na City of Griffin v americkej Georgii viedol k presmerovaniu dvoch platieb a strate pre mesto vo výške 800 000 USD.**

- **Marylandský úrad práce utrpel prienik do svojej databázy. Útočníci pristúpili k osobným údajom 78 000 osôb.**

- **Voľne dostupný Jenkins server spoločnosti GE Aviation poskytoval prístup k zdrojovým kódom, heslám, privátnym kľúčom a konfiguračným nastaveniam systémov, vnútornej infraštruktúre spoločnosti.**

- **Nezabezpečená ElasticSearch databáza oddelenia verejnej bezpečnosti čínskej provincie Jiangsu umožňovala prístup k osobným údajom 90 miliónov ľudí, aj obchodným dátam.**

- **Malvér napadol systémy okresu LaPorte v Indiane, USA, vrátane e-mailov. Jednalo**

sa o ďalší z radu ransomvérových útokov, pričom útočníci použili Ryuk. Mesto zaplatilo 130 000 USD.

- Spyware FinSpy / FinFisher, ktorý vyvíja nemecká spoločnosť Gamma International pre vlády, objavený v Mjanmarsku. Obetiam kradne citlivé dáta z mobilných zaraidení.

- 25 miliónov zariadení Android infikovaných malvérom nazvaným Agent Smith. Zamieňa legitímne aplikácie za infikované verzie a zobrazuje nevyžiadané reklamy.

- Prienik na archivačný server webového prehliadača Pale Moon. Útočníci infikovali archivované verzie inštalátorov prehliadača až po 27.6.2.

- Ransomvér odstavil servery všetkých fakúlt Monroe College v New Yorku. Útočníci za dekryptovací kľúč pýtajú 2 milióny USD.

- Telekomunikačná spoločnosť Sprint dvakrát po sebe napadnutá. Útočníci využili stránku samsung.com a mohli pristúpiť k citlivým dátam klientov.

- Zraniteľnosť tisícok výbehových úložísk Iomega/LenovoEMC dovoľovala prístup k 3 miliónom súborov vrátane citlivých dát. Spoločnosť Lenovo chybu opravila v troch zraniteľných verziách svojho softvéru.

- Nezabezpečená Elasticsearch databáza neznámej firmy uložená na Elastic klastri spoločnosti Aliyun Computing Co (Alibaba Cloud) dovoľoval prístup k citlivým údajom a údajom o polohe miliónov čínskych používateľov.

- Občania Kazachstanu majú od júla povinnosť inštalovať si do každého zariadenia vládny certifikát na dešifrovanie HTTPS prenosu a jeho opätovné šifrovanie po kontrole.

- Výskumníci zistili, že 93% z takmer 22 500 stránok pre dospelých poskytuje dáta svojich návštevníkov tretím stranám.

- Bezpečnostná spoločnosť FireEye oznámila, že iránska skupina APT34 OilRig začala používať tri nové rodiny malvéru.

- Nový druh ransomvéru obmedzil služby cloudového poskytovateľa iNSYNQ. Zálohy ostali istý čas nedostupné kvôli riziku ich infekcie.

- Twitterový účet, e-maily a webstránky tlačovej agentúry britskej polície Scotland Yard napadnuté, útočníci uverejňovali zvláštne odkazy.

- Čínska skupina APT15 používa nové zadné vrátka, informovala spoločnosť ESET.

- **62 amerických univerzít utrpelo prienik do svojich systémov. Na vine bola zraniteľnosť administračného systému Banner Web Tailor.**

- **13-dňového DDoS útoku na steamingovú aplikáciu sa zúčastnilo vyše 400 000 jedinečných IP adries.**

- **Na Darknete sa predáva 23 miliónov ukradnutých kreditných kariet. Najčastejšie z Británie a USA.**

- **Louisiana vyhlásila výnimočný stav po útoku ransomvérom na tri školské okruhy.**

- **Uväznili štyroch útočníkov, ktorí sa nabúrali do vyše 1000 účtov komunikačnej aplikácie Telegram, vrátane účtov brazílskeho prezidenta a ministrov.**

- **Polícia Los Angeles (LAPD) utrpela prienik do svojich systémov. Unikli osobné údaje zhruba 2500 príslušníkov a 17 500 žiadateľov o zamestnanie v zbore.**

- **Odcudzené prihlasovacie údaje ku 4 miliónom účtov online hry Club Penguin Rewritten. Útočníci hľadali cenné účty a chceli zničiť záznamy; administrátori odporúčajú používateľom zmenu hesla.**

- **Nezabezpečená Elasticsearch databáza umožňovala prístup k údajom 300 000 zamestnancov spoločnosti Honda a informáciám o ich firemných počítačoch, vrátane informácií o ich zabezpečení, či jeho nedostatku.**

Závažné zraniteľnosti bežných softvérových produktov

Zraniteľnosť SACK Panic spôsobuje zrútenie linuxového systému

Spoločnosť Netflix zverejnila informácie o štyroch zraniteľnostiach v jadre operačného systému Linux, ktoré označila ako kritické. Zraniteľnosti súvisia s funkcionalitou TCP protokolu a nachádzajú sa v mechanizme SACK a parametri MSS. Útočník môže spôsobiť neúmerné vyťaženie systémových prostriedkov a nedostupnosť systému.

Kritická zraniteľnosť Drupal 8.7.4 umožňuje prevziať kontrolu nad webstránkou

Kritická zraniteľnosť v manažéri obsahu webstránok Drupal umožňuje útočníkom pri návšteve stránky obísť autentifikáciu a získať nad ňou plnú kontrolu. Je spojená s modulom Workspaces. Zraniteľná je verzia Drupal 8.7.4.

Palo Alto - kritická zraniteľnosť umožňuje vzdialene vykonávať kód

V produktoch Palo Alto Networks GlobalProtect a GlobalProtect Gateway bola objavené kritická zraniteľnosť umožňujúca útočníkom vzdialene vykonávať kód. K tomu stačí poslať zraniteľnému zariadeniu špeciálne upravenú požiadavku, nakoľko používateľský vstup nie je vhodne ošetrený. Útočník nepotrebuje autentifikáciu.

Kritická zraniteľnosť VLC Media Player

V multimediálnom prehrávači VLC Media Player bola nájdená kritická zraniteľnosť, ktorá útočníkom umožňuje prevziať kontrolu nad zraniteľným zariadením, vykonávať na ňom vzdialene kód, spôsobiť nedostupnosť jeho služieb, pristupovať k súborom a informáciám a manipulovať s nimi. K tomu nie sú potrebné systémové oprávnenia, ani interakcia obete.

Kritická zraniteľnosť Androidov umožňuje prevzatie kontroly nad zariadením

Systémy Android vo verziách 7 až 9 obsahujú kritickú zraniteľnosť, ktorú môže útočník zneužiť na vzdialené vykonávanie kódu privilegovaného procesu a prevzatie kontroly nad zariadením. Chyba umožňujúca zápis mimo povolenú hodnotu sa konkrétne nachádza v prehrávači Android Player a zneužiteľná je po spustení škodlivého video súboru.

Kritické zraniteľnosti produktov Cisco

V produktoch Cisco bolo opravených viacero rozličných kritických a závažných zraniteľností:
Cisco DNA Center (CVE-2019-1848): zraniteľnosť spôsobená nedostatočným obmedzením prístupov k systémovým portom umožňuje obísť autentifikáciu a získať prístup ku kritickým interným systémom.
Cisco Data Center Network Manager (CVE-2019-1619): kvôli nesprávnemu manažovaniu relácií je možné získať ku zraniteľnému zariadeniu administrátorský prístup.
Cisco Data Center Network Manager (CVE-2019-1620): kvôli nesprávnemu nastaveniu oprávnení je možné nahrať na zraniteľné zariadenie ľubovoľné súbory a vykonávať kód s právami root.
Cisco ASA and FTD Software Cryptographic TLS and SSL Driver (CVE-2019-1620): nesprávne vyhodnocovanie vstupov SSL / TLS hlavičiek prichádzajúcich paketov dovoľuje poslať upravený paket, ktorý spôsobí reštart zariadenia a teda DoS podmienky.
Cisco Identity Services Engine (CVE-2019-1942): kvôli nedostatočnému ošetreniu používateľských vstupov umožňuje aplikácia prístup k dátam, ich modifikáciu a zneužívanie ďalších zraniteľností databázy využitím SQL injekcie.
Cisco IOS Access Points Software (CVE-2019-1920): kvôli nevhodnému narábaniu s chybami klientskych autentifikačných požiadaviek je možné spôsobiť nedostupnosť systému (DoS).

Kritická zraniteľnosť Wireshark umožňuje DoS útok

V nástroji Wireshark bola objavená zraniteľnosť CVE-2019-13619, ktorá umožňuje vyvolať nedostupnosť aplikácie (DoS). Na to je potrebné injektovať škodlivý paket, alebo presvedčiť obeť, aby prečítala škodlivý paket trace súbor. Zraniteľnosť súvisí so súborom epan/asn1.c.

Chyba v platforme Docker umožňuje únik informácií

Platforma pre vývoj, dodanie a beh aplikácií Docker CE a EE obsahuje zraniteľnosť, ktorá s debug móde umožňuje únik informácií. Je spojená s presúvaním zásobníka obsahujúceho citlivé údaje pomocou príkazu „docker stack deploy“. Útočník sa tak môže dostať k tajomstvám uloženým v debug logu.

Zraniteľnosť ProFTPD umožňuje vzdialene vykonávať kód

FTP platforma ProFTPD umožňovala za istých podmienok vzdialene vykonávať kód a exfiltrovať informácie. Zraniteľnosť sa nachádzala v príkazoch SITE CPFR a SITE CPTO, ktoré nebrali do úvahy zákaz zapisovania súborov do pracovnej zložky, ani v prípade, že používateľ nemal oprávnenia.

Urgent/11 – súbor kritických zraniteľností ohrozujúcich 200 miliónov zariadení

Kritické zraniteľnosti v operačnom systéme VxWorks, ktoré objavili výskumníci spoločnosti Armis, ohrozujú približne 200 miliónov IoT zariadení. Jedná sa o 11 zraniteľností nazvaných súhrnne Urgent/11, ktoré sa nachádzajú v implementácii sieťového protokolu TCP/IP (IPnet). 6 z nich umožňuje vykonávanie ľubovoľného kódu a prevzatie kontroly nad zraniteľným zariadením. Systém VxWorks používajú zariadenia IoT, medzi inými aj firewally, routre, MRI, výťahy a SCADA systémy.

Mesačník zraniteľností Júl 2019

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

TLP: White

5. Frameworky
    - Microsoft .NET Framework
    - Oracle Java
6. Iné tohtomesačné závažné zraniteľnosti
    - Linuxové jadro
    - Drupal
    - Palo Alto
    - Systémy Android

https://www.csirt.gov.sk/aktualne-7d7.html?id=198