BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 08. 2018 – 14. 08. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Delta Electronics CNCSoft and ScreenEditor Vulnerabilities

Popis

Spoločnosť Delta Electronics vydala bezpečnostné aktualizácie na svoje produkty CNCSoft a ScreenEditor, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

07.08.2018

CVE

CVE-2018-10636, CVE-2018-10598

Zasiahnuté systémy

CNCSoft verzie staršie ako 1.01.09
ScreenEditor verzia 1.00.54

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-219-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Adobe Acrobat and Reader Vulnerabilities

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje produkty Adobe Acrobat a Reader, ktoré opravujú viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované bezpečnostné zraniteľnosti sú umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

14.08.2018

CVE

CVE-2018-12799, CVE-2018-12808

Zasiahnuté systémy

Adobe Acrobat DC pre Windows a MacOS verzia 2018.011.20055 a staršie
Adobe Acrobat Reader DC (Continuous Track) pre Windows a MacOS verzia 2018.011.20055 a staršie
Adobe Acrobat 2017 pre Windows a MacOS verzia 2017.011.30096 a staršie
Adobe Acrobat Reader 2017 (Classic 2017 Track) pre Windows a MacOS verzia 2017.011.30096 a staršie
Adobe Acrobat DC (Classic 2015 Track) pre Windows a MacOS verzia 2015.006.30434 a staršie
Adobe Acrobat Reader DC (Classic 2015 Track) pre Windows a MacOS verzia 2015.006.30434 a staršie
Acrobat Reader 2017 verzia 2017.011.30066 a staršie pre Windows a MacOS

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a súbory z neznámych zdrojov.

Zdroje

https://helpx.adobe.com/security/products/acrobat/apsb18-29.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.9**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Intel Side-Channel L1TF (Foreshadow) Vulnerabilities

Popis

Spoločnosť Intel vydala oznámenie o bezpečnostných zraniteľnostiach vo svojich procesoroch radu Intel Core a Intel Xeon.
Bezpečnostné zraniteľnosti zneužívajú optimalizačnú techniku procesorov známu ako "speculative execution" a tiež funkciu Intel® software guard extensions (Intel® SGX) a umožňujú lokálnemu neautentifikovanému útočníkovi prostredníctvom side-channel analýzy získať prístup k citlivým údajom uloženým v L1 cache pamäti procesora.

Dátum prvého zverejnenia varovania

14.08.2018

CVE

CVE-2018-3615, CVE-2018-3620, CVE-2018-3646

Zasiahnuté systémy

Intel® Core™ i3 processor (45nm and 32nm)
Intel® Core™ i5 processor (45nm and 32nm)
Intel® Core™ i7 processor (45nm and 32nm)
Intel® Core™ M processor family (45nm and 32nm)
2nd generation Intel® Core™ processors
3rd generation Intel® Core™ processors
4th generation Intel® Core™ processors
5th generation Intel® Core™ processors
6th generation Intel® Core™ processors
7th generation Intel® Core™ processors
8th generation Intel® Core™ processors
Intel® Core™ X-series Processor Family for Intel® X99 platforms
Intel® Core™ X-series Processor Family for Intel® X299 platforms
Intel® Xeon® processor 3400 series
Intel® Xeon® processor 3600 series
Intel® Xeon® processor 5500 series
Intel® Xeon® processor 5600 series
Intel® Xeon® processor 6500 series
Intel® Xeon® processor 7500 series
Intel® Xeon® Processor E3 Family
Intel® Xeon® Processor E3 v2 Family
Intel® Xeon® Processor E3 v3 Family
Intel® Xeon® Processor E3 v4 Family

Intel® Xeon® Processor E3 v5 Family
Intel® Xeon® Processor E3 v6 Family
Intel® Xeon® Processor E5 Family
Intel® Xeon® Processor E5 v2 Family
Intel® Xeon® Processor E5 v3 Family
Intel® Xeon® Processor E5 v4 Family
Intel® Xeon® Processor E7 Family
Intel® Xeon® Processor E7 v2 Family
Intel® Xeon® Processor E7 v3 Family
Intel® Xeon® Processor E7 v4 Family
Intel® Xeon® Processor Scalable Family
Intel® Xeon® Processor D (1500, 2100)

Následky
Neoprávnený prístup k citlivým údajom

Odporúčania
Spoločnosť Intel spolupracovala s vývojármi operačných systémov a firmvérov na vydaní softvérových bezpečnostných záplat. Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html https://foreshadowattack.eu/ https://www.bleepingcomputer.com/news/security/researchers-disclose-new-foreshadow-l1tf-vulnerabilities-affecting-intel-cpus/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BIND DoS Vulnerability

Popis

Vývojári DNS servera BIND vydali aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť spôsobenú chybou vo funkcii "deny-answer-aliases".
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na vyvolanie chyby v komponente INSIST a následné zneprístupnenie služby.
Funkcia "deny-answer-aliases" je v natívnej konfigurácii servera vypnutá.

Dátum prvého zverejnenia varovania

08.08.2018

CVE

CVE-2018-5740

Zasiahnuté systémy

BIND verzie staršie ako 9.9.13-P1, 9.10.8-P1, 9.11.4-P1, 9.12.2-P1 a 9.11.3-S3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame vypnúť funkciu "deny-answer-aliases".

Zdroje

https://kb.isc.org/article/AA-01639/0

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Rosenbridge Backdoor Mechanism in VIA C3 x86 Processors

Popis

Výskumník zverejnil podrobnosti o novoobjavenej zraniteľnosti v procesoroch VIA C3 produkovaných spoločnosťou Via Technologies v rokoch 2001 až 2003. Bezpečnostná zraniteľnosť spočíva v chýbajúcich autentifikačných mechanizmoch v koprocesore RISC (Reduced Instruction Set Computer), ktorý je voľne prístupný v niektorých verziách systému. Zraniteľnosť umožňuje útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.08.2018

CVE

-

Zasiahnuté systémy

Procesory Via Technologies VIA C3 x86

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Používateľom zasiahnutých systémov odporúčame ich nahradenie alternatívnymi produktami.

Zdroje

https://github.com/xoreaxeaxeax/rosenbridge
https://www.bleepingcomputer.com/news/security/backdoor-mechanism-discovered-in-via-c3-x86-processors/
https://www.theregister.co.uk/2018/08/10/via_c3_x86_processor_backdoor/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Philips IntelliSpace Cardiovascular Vulnerabilities

Popis

Spoločnosť Philips vydala oznámenie o viacerých bezpečnostných zraniteľnostiach vo svojich produktoch Philips' IntelliSpace Cardiovascular a Xcelera.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu autentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

14.08.2018

CVE

CVE-2018-14787, CVE-2018-14789

Zasiahnuté systémy

IntelliSpace Cardiovascular, verzia 3.1 a staršie
Xcelera verzia 4.1 a staršie

Následky

Vykonanie škodlivého kódu

Odporúčania

Spoločnosť Philips doposiaľ nevydala bezpečnostné aktualizácie uvedených produktov. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu softvéru.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-226-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

New attack vector on WPA/WPA2 using PMKID

Popis

Výskumník projektu Hashcat zverejnil podrobnosti o novoobjavenom útočnom vektore, prostredníctvom ktorého možno získať prístup ku WiFi WPA/WPA2 komunikácii zabezpečenej zdieľanými kľúčmi PSK. Útočný vektor spočíva v pasívnom odpočúvaní komunikácie pri nadväzovaní spojenia Extensible Authentication Protocol over LAN (EAPOL), pričom na úspešný útok postačuje zachytiť jediný rámec obsahujúci Robust Security Network-Pairwise Master Key Identification (RSN-PMKID) sekvenciu. Nakoľko táto je totožná so zdieľaným kľúčom PSK, jej rozšifrovaním získa útočník prístup ku sieťovej komunikácii.

Dátum prvého zverejnenia varovania

04.08.2018

CVE

-

Zasiahnuté systémy

Technológia Wi-Fi Protected Access (WPA) a Wi-Fi Protected Access 2 (WPA2) využívajúca autentifikáciu zdieľanými kľúčmi PSK

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na zabezpečenie WiFi komunikácie odporúčame namiesto zdieľaných kľúčov PSK využívať autentifikačné mechanizmy štandardu 802.1x. V prípade použitia zdieľaných kľúčov PSK odporúčame nastaviť silné heslá čo najväčšej dĺžky.

Zdroje

https://hashcat.net/forum/thread-7717.html
https://thehackernews.com/2018/08/how-to-hack-wifi-password.html
https://www.theregister.co.uk/2018/08/06/wpa2_wifi_pmkid_hashcat/
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180809-wpa2

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Medtronic MiniMed Insulin Pump Vulnerabilities

Popis

Spoločnosť Medtronic vydala oznámenie o viacerých bezpečnostných zraniteľnostiach vo svojich inzulínových pumpách MiniMed.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente zachytiť a replikovať komunikáciu medzi diaľkovým ovládačom a pumpou (Man-in-the-middle útok).

Dátum prvého zverejnenia varovania

07.08.2018

CVE

CVE-2018-10634, CVE-2018-14781

Zasiahnuté systémy

Medtronic MiniMed - 508 MiniMed
Medtronic MiniMed - 522 / MMT - 722 Paradigm REAL-TIME,
Medtronic MiniMed - 523 / MMT - 723 Paradigm Revel,
Medtronic MiniMed - 523K / MMT - 723K Paradigm Revel
Medtronic MiniMed - 551 / MMT - 751 MiniMed 530G

Následky

Neoprávnený prístup do systému

Odporúčania

Spoločnosť Medtronic nevydá aktualizácie pre zasiahnuté produkty. Zraniteľnosti sú zneužiteľné pri používaní diaľkového ovládača a povolení funkcií "easy bolus" a "remote bolus", ktoré sú v základnom nastavení vypnuté. Administrátorom a používateľom odporúčame v zariadení vypnúť funkcie "easy bolus" a "remote bolus" a nepoužívať diaľkový ovládač ku zariadeniu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-219-02