BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 06. 2018 – 19. 06. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

SK-CERT
Naša značka:
02049/2018/TS/OKB-074

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

Identifikátor

Microsoft Releases June 2018 Security Updates

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú 51 bezpečnostných zraniteľností.
Najzávažnejšie sú zraniteľnosti v skriptovacích enginoch využívaných v internetových prehliadačoch Edge a Internet Explorer, spočívajú v nesprávnom spracovaní objektov v pamäti a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu v kontexte prihláseného používateľa.

Dátum prvého zverejnenia varovania

12.06.2018

CVE

CVE-2018-0871, CVE-2018-0978, CVE-2018-0982, CVE-2018-1036, CVE-2018-1040, CVE-2018-8110, CVE-2018-8111, CVE-2018-8113, CVE-2018-8121, CVE-2018-8140, CVE-2018-8169, CVE-2018-8175, CVE-2018-8201, CVE-2018-8205, CVE-2018-8207, CVE-2018-8208, CVE-2018-8209, CVE-2018-8210, CVE-2018-8210, CVE-2018-8211, CVE-2018-8212, CVE-2018-8213, CVE-2018-8214, CVE-2018-8215, CVE-2018-8216, CVE-2018-8217, CVE-2018-8218, CVE-2018-8219, CVE-2018-8221, CVE-2018-8224, CVE-2018-8225, CVE-2018-8226, CVE-2018-8227, CVE-2018-8229, CVE-2018-8231, CVE-2018-8233, CVE-2018-8234, CVE-2018-8235, CVE-2018-8236, CVE-2018-8239, CVE-2018-8243, CVE-2018-8244, CVE-2018-8245, CVE-2018-8246, CVE-2018-8247, CVE-2018-8248, CVE-2018-8249, CVE-2018-8251, CVE-2018-8252, CVE-2018-8254, CVE-2018-8267

Zasiahnuté systémy

Internet Explorer, Microsoft Edge, Microsoft Windows, Microsoft Office and Microsoft Office Services and Web Apps, ChakraCore, Adobe Flash Player

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/7d4489d6-573f-e811-a96f-000d3a33c573
https://blog.talosintelligence.com/2018/06/ms-tuesday.html

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

Identifikátor

Google Stable Channel Update for Desktop June 2018

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje viacero chýb a bezpečnostnú zraniteľnosť v komponente JavaScript Interpreter (Chrome V8).
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

12.06.2018

CVE

CVE-2018-6149

Zasiahnuté systémy

Google Chrome verzie staršie ako 67.0.3396.87

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://chromereleases.googleblog.com/2018/06/stable-channel-update-for-desktop_12.html
https://www.securitytracker.com/id/1041123s

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

Identifikátor

Vulnerabilities in RAPIDLab 1200 and RAPIDPoint 400/500 Blood Gas Analyzers

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na analyzátory krvných plynov RAPIDLab 1200 and RAPIDPoint 400/500, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov vo funkcii "*remote view*" a vzdialený autentifikovaný útočník by ju mohol zneužiť na eskaláciu svojich privilégií.
Druhá bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie prístupu do systému zariadenia prostredníctvom portu 5900/TCP.

Dátum prvého zverejnenia varovania

12.06.2018

CVE

CVE-2018-4845, CVE-2018-4846

Zasiahnuté systémy

RAPIDLab 1200
RAPIDPoint 400, 405, 500

Následky

Eskalácia privilégií, Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Taktiež odporúčame limitovať fyzický prístup k zariadeniam a zakázať funkciu "remote view" v nastaveniach zariadení.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-755010.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.7**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Security Notice for CA Privileged Access Manager

Popis

Spoločnosť CA Technologies vydala bezpečnostnú aktualizáciu na svoj produkt CA Privileged Access Manager, ktorá opravuje 15 bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a nedostatočnom overovaní používateľských vstupov vo viacerých skriptoch (*ajax_cmd.php, login.php, update_crld, read_sessionlog.php*). Vzdialený neautentifikovaný útočník by zraniteľnosti mohol zneužiť na získanie administrátorských práv a vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.06.2018

CVE

CVE-2018-9021, CVE-2018-9022, CVE-2018-9023, CVE-2018-9024, CVE-2018-9025, CVE-2018-9026, CVE-2018-9027, CVE-2015-4664, CVE-2015-4665, CVE-2015-4666, CVE-2015-4667, CVE-2015-4669, CVE-2015-4668, CVE-2018-9028, CVE-2018-9029

Zasiahnuté systémy

CA Privileged Access Manager verzie staršie ako 3.0.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://communities.ca.com/docs/DOC-231182267-ca20180614-01-security-notice-for-ca-privileged-access-manager
https://www.cybersecurity-help.cz/vdb/SB2018061508

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SAP Security Patch Day – June 2018

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti nachádzajúce sa v produktoch SAP Business One a SAP Internet Sales by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby alebo neoprávnený prístup k citlivým údajom (systémové dáta, zdrojové kódy, konfiguračné súbory).

Dátum prvého zverejnenia varovania

12.06.2018

CVE

CVE-2014-0050, CVE-2015-0899, CVE-2018-2408, CVE-2018-2416, CVE-2018-2424, CVE-2018-2425, CVE-2018-2428

Zasiahnuté systémy

SAP Business One for SAP HANA Backup Service
SAP Internet Sales
SAP Business Objects
SAP CMC/BI Launchpad/Fiorified BI Launchpad
SAP CrystalReports
SAPUI5
UI5 Handler
SAP Identity Management

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=495289255
https://erpscan.com/press-center/blog/sap-cyber-threat-intelligence-report-june-2018/

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

Identifikátor

Multiple Vulnerabilities in Siemens Products

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch SCALANCE X, RUGGEDCOM WiMAX, RFID 181-EIP a SIMATIC RF182C.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní DHCP odpovedí a útočník nachádzajúci sa v rovnakom sieťovom segmente by ju prostredníctvom podvrhnutia špeciálne vytvorenej DHCP odpovede mohol zneužiť na vykonanie škodlivého kódu. Uvedenú zraniteľnosť je možné zneužiť na všetkých produktoch uvedených v časti zasiahnuté systémy.
Ďalšie zraniteľnosti v prepínačoch série SCALANCE spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený útočník by ich mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

12.06.2018

CVE

CVE-2018-4833, CVE-2018-4842, CVE-2018-4848

Zasiahnuté systémy

Siemens SCALANCE X-200 verzie staršie ako v5.2.3
Siemens SCALANCE X-200 IRT verzie staršie ako v5.4.1
Siemens SCALANCE X-300 všetky verzie
Siemens RFID 181-EIP všetky verzie
Siemens RUGGEDCOM WiMAX v4.4 a v4.5
Siemens X-204RNA všetky verzie
Siemens SCALANCE X408, X414 všetky verzie
Siemens SIMATIC RF182C všetky verzie

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://cert-portal.siemens.com/productcert/txt/ssa-181018.txt
https://cert-portal.siemens.com/productcert/txt/ssa-480829.txt

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

Identifikátor

Multiple Vulnerabilities in SCALANCE M875

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj produkt SCALANCE M875, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšie zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov webového rozhrania a vzdialený autentifikovaný útočník by ich mohol zneužiť na vykonanie škodlivého kódu.
Ďalšiu zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom CSRF (Cross-Site Request Forgery) útoku mohol zneužiť na vykonanie príkazov v kontexte prihláseného používateľa.
Ostatné zraniteľnosti by útočník mohol zneužiť na neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.06.2018

CVE

CVE-2018-4859, CVE-2018-4860, CVE-2018-4861, CVE-2018-11447, CVE-2018-11448, CVE-2018-11449

Zasiahnuté systémy

SCALANCE M875

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-977428.pdf

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

Identifikátor

RSA Authentication Manager XSS Vulnerabilities

Popis

Spoločnosť RSA vydala bezpečnostnú aktualizáciu na svoj produkt RSA Authentication Manager, ktorá opravuje viacero bezpečnostných zraniteľností v komponentoch Operations Console a Security Console.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnom filtrovaní HTML kódu v používateľských vstupoch a vzdialený neautentifikovaný útočník by ich mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.

Dátum prvého zverejnenia varovania

15.06.2018

CVE

CVE-2018-1253, CVE-2018-1254

Zasiahnuté systémy

RSA Authentication Manager verzie staršie ako 8.3 P1

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://securitytracker.com/id/1041134
https://packetstormsecurity.com/files/148197/DSA-2018-107.txt
https://exchange.xforce.ibmcloud.com/vulnerabilities/144860
https://exchange.xforce.ibmcloud.com/vulnerabilities/144861

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

Identifikátor

BIND Recursive Query Vulnerability

Popis

Vývojári DNS servera BIND vydali upozornenie na bezpečnostnú zraniteľnosť svojho produktu, ktorá umožňuje všetkým klientom vykonávať rekurzívne dopyty na DNS server. Bezpečnostná zraniteľnosť spočíva v nesprávnej implementácii bezpečnostných mechanizmov riadenia prístupu klientov k funkcii *recursive query* a vzdialený útočník by ju mohol zneužiť na získanie neoprávneného prístupu k výsledkom dopytov uložených v cache pamäti servera alebo na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.06.2018

CVE

CVE-2018-5738

Zasiahnuté systémy

BIND verzie 9.9.12, 9.10.7, 9.11.3, 9.12.0->9.12.1-P2, 9.13.0, 9.9.12-S1, 9.10.7-S1, 9.11.3-S1, a 9.11.3-S2

Následky

Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Ak server nemusí vykonávať rekurzívne dopyty, administrátorom odporúčame vypnúť funkciu *recursive query* v *named.conf* nastavením príznaku *"recursion no;"*. V prípade, ak chcete využívať funkciu *recursive query*, odporúčame ju špecificky zadefinovať prostredníctvom direktívy *allow-recursion*. Tiež odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://kb.isc.org/article/AA-01616
https://securitytracker.com/id/1041115