BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 04. 2020 - 14. 04. 2020

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:
01439/2020/SK-CERT-084

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.04.2020

CVE

CVE-2020-6423, CVE-2020-6430, CVE-2020-6431, CVE-2020-6432, CVE-2020-6433, CVE-2020-6434, CVE-2020-6435, CVE-2020-6436, CVE-2020-6437, CVE-2020-6438, CVE-2020-6439, CVE-2020-6440, CVE-2020-6441, CVE-2020-6442, CVE-2020-6443, CVE-2020-6444, CVE-2020-6445, CVE-2020-6446, CVE-2020-6447, CVE-2020-6448, CVE-2020-6454, CVE-2020-6455, CVE-2020-6456

Zasiahnuté systémy

Google Chrome verzie staršie ako 81.0.4044.92

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, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_7.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/179206

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

Identifikátor

Mozilla Firefox viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox a Firefox ESR, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.04.2020

CVE

CVE-2020-6821, CVE-2020-6822, CVE-2020-6823, CVE-2020-6824, CVE-2020-6825, CVE-2020-6826, CVE-2020-6827, CVE-2020-6828

Zasiahnuté systémy

Firefox verzie staršie ako 75
Firefox ESR verzie staršie ako 68.7

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, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2020-12/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-13/
https://exchange.xforce.ibmcloud.com/vulnerabilities/179179
https://exchange.xforce.ibmcloud.com/vulnerabilities/179180

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

Identifikátor

Amcrest/Dahua IP kamery a NVR zraniteľnosti

Popis

Spoločnosť Amcrest vydala bezpečnostné aktualizácie na svoje IP kamery a NVR zariadenia, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov na porte 37777 a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom brute force útoku získať neoprávnený prístup do systému.
Na uvedené zraniteľnosti je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

07.04.2020

CVE

CVE-2020-5735, CVE-2020-5736

Zasiahnuté systémy

IP2M-853EW
IP2M-858W
IP4M-1053EW
IP2M-866W
IP2M-866EW
- verzie staršie ako:
Amcrest_SD-Mao-Rhea_Eng_N_Stream3_AMCREST_V2.623.00AC004.0.R.200316.bin

AMDV10814-H5
- verzie staršie ako:
Amcrest_XVR5x04-X1_Eng_N_Amcrest_V4.000.00AC000.0.R.200218.bin

IP2M-841
IPM-721
IPM-HX1
- verzie staršie ako:
Amcrest_IPC-AWXX_Eng_N_AMCREST_V2.420.AC00.18.R.20200217.bin

IP8M-2597E
- verzie staršie ako:
Amcrest_IPC-HX2(1)XXX-Sag_Eng_N_AMCREST_V2.800.00AC000.0.R.200330.bin

IP2M-841-V3
- verzie staršie ako:
Amcrest_IPC-Consumer-Web-Mao-Molec_Eng_N_AMCREST_V2.800.0000000.6.R.200314.bin

IP8M-2493EB
IP8M-2496EB
IP8M-2454EW
IP8M-T2499EW
IP8M-MT2544EW
IP8M-MB2546EW
- verzie staršie ako:
Amcrest_IPC-HX5X3X-Rhea_Eng_NP_Stream3_AMCREST_V2.622.00AC000.0.R.200320.bin

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame uistiť sa, že zariadenia nie sú prístupné z internetu na porte 37777.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.tenable.com/security/research/tra-2020-20

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

Identifikátor

Rockwell Automation RSLinx Classic zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt RSLinx Classic, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.04.2020

CVE

CVE-2020-10642

Zasiahnuté systémy

Rockwell Automation RSLinx Classic 3.60 až 4.11 verzie staršie ako patch 1091155

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-20-100-01
https://exchange.xforce.ibmcloud.com/vulnerabilities/179373

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell produkty bezpečnostná zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoje produkty Dell X-Series, PC5500 a VRTX, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených požiadaviek získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

09.04.2020

CVE

CVE-2020-5330

Zasiahnuté systémy

Dell X-Series firmware verzie 3.0.1.2 a staršie
Dell PC5500 firmware verzie 4.1.0.22 a staršie
Dell VRTX Switch Modules firmware verzie 2.0.0.77 a staršie

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.dell.com/support/article/sk-sk/sln320366/dsa-2020-042-dell-networking-security-update-for-an-information-disclosure-vulnerability?lang=en
https://nvd.nist.gov/vuln/detail/CVE-2020-5330
https://exchange.xforce.ibmcloud.com/vulnerabilities/179464

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Fuji Electric V-Server Lite zraniteľnosť

Popis

Spoločnosť Fuji Electric vydala bezpečnostnú aktualizáciu na svoj produkt V-Server Lite, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených VPR súborov spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.04.2020

CVE

CVE-2020-10646

Zasiahnuté systémy

Fuji Electric V-Server Lite verzie staršie ako 4.0.9.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-20-098-04