BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 10. 2018 - 23. 10. 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-171

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

Identifikátor

Google Chrome Stable Channel Update

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností v internetovom prehliadači Google Chrome.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu v kontexte webového prehliadača a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.10.2018

CVE

CVE-2018-17462, CVE-2018-17463, CVE-2018-17464, CVE-2018-17465, CVE-2018-17466, CVE-2018-17467, CVE-2018-17468, CVE-2018-17469, CVE-2018-17470, CVE-2018-17471, CVE-2018-17472, CVE-2018-17473, CVE-2018-17474, CVE-2018-17475, CVE-2018-17476, CVE-2018-17477, CVE-2018-5179

Zasiahnuté systémy

Google Chrome verzie staršie ako 70.0.3538.67

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2018/10/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2018-116/

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

Identifikátor

Adobe Digital Editions zraniteľnosti

Popis

Spoločnosť Adobe vydala aktualizáciu svojho produktu Adobe Digital Editions, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

09.10.2018

CVE

CVE-2018-12813, CVE-2018-12814, CVE-2018-12816, CVE-2018-12818, CVE-2018-12819, CVE-2018-12820, CVE-2018-12821, CVE-2018-12822, CVE-2018-12823

Zasiahnuté systémy

Adobe Digital Editions 4.5.8 a staršie

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.

Zdroje

=https://helpx.adobe.com/security/products/Digital-Editions/apsb18-27.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/151008

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

Identifikátor

Opto 22 PAC Control Basic a PAC Control Professional zraniteľnosť

Popis

Spoločnost Opto 22 vydala bezpečnostné aktualizácie na svoje produkty PAC Control Basic a PAC Control Professional, ktoré opravujú bezpečnostnú zraniteľnosť. Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje lokálnemu útočníkovi spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

18.10.2018

CVE

CVE-2018-14807

Zasiahnuté systémy

Opto 22 PAC Control Basic a PAC Control Professional verzie R10.0a a staršie

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-14807
https://ics-cert.us-cert.gov/advisories/ICSA-18-247-01
https://www.opto22.com/support/resources-tools/knowledgebase/kb87547

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

Identifikátor

Adobe Framemaker zraniteľnosť

Popis

Spoločnosť Adobe vydala aktualizáciu svojho produktu Adobe Framemaker, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním DLL súborov a umožňuje lokálnemu neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov eskalovať svoje privilégia na napadnutom systéme.

Dátum prvého zverejnenia varovania

09.10.2018

CVE

CVE-2018-15974

Zasiahnuté systémy

Adobe Framemaker verzia 14.0.361 a staršie

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/framemaker/apsb18-37.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/151002

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

Identifikátor

Dell EMC Secure Remote Services Virtual Edition viacero zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie na svoj produkt Dell EMC Secure Remote Services Virtual Edition, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

15.10.2018

CVE

CVE-2018-11079, CVE-2018-11080, CVE-2018-15765

Zasiahnuté systémy

Dell EMC Secure Remote Services Virtual Edition verzie staršie ako 3.32.00.08

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.

Zdroje

https://seclists.org/fulldisclosure/2018/Oct/35

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Omron CX-Supervisor zraniteľnosť

Popis

Vývojári spoločnosti Omron vydali bezpečnostnú aktualizáciu svojho produktu CX-Supervisor, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nesprávnom spracovaní konvertovaných súborov zasiahnutým systémom a umožňuje lokálnemu útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

17.10.2018

CVE

CVE-2018-17905, CVE-2018-17907, CVE-2018-17909, CVE-2018-17913

Zasiahnuté systémy

Omron CX-Supervisor verzie staršie ako 3.4.2

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-290-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.9
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť vo VMware produktoch

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoje produkty vSphere ESXi, Workstation a Fusion, ktorá opravuje bezpečnostnú zraniteľnosť v komponente SVDA.
Bezpečnostná zraniteľnosť umožňuje lokálnemu útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

16.10.2018

CVE

CVE-2018-6974

Zasiahnuté systémy

VMware vSphere ESXi (ESXi) verzie staršie ako 6.0, 6.5 a 6.7
VMware Workstation Pro / Player (Workstation) verzie staršie ako 14.1.3
VMware Fusion Pro, Fusion (Fusion) verzie staršie ako 14.1.3

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0026.html
https://www.securitytracker.com/id/1041876
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6974

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

Identifikátor

Adobe Experience Manager zraniteľnosti

Popis

Spoločnosť Adobe vydala aktualizácie svojho produktu Adobe Experience Manager, ktoré riešia viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú lokálnemu autentifikovanému útočníkovi prostredníctvom XSS útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

09.10.2018

CVE

CVE-2018-15969, CVE-2018-15970, CVE-2018-15971, CVE-2018-15972, CVE-2018-15973

Zasiahnuté systémy

Adobe Experience Manager verzie 6.0 až 6.4

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www.securityfocus.com/bid/105576
https://helpx.adobe.com/security/products/experience-manager/apsb18-36.html
https://www.cybersecurity-help.cz/vdb/SB2018101012