BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 04. 2019 - 16. 04. 2019

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:
01380/2019/TS/OKB-114

BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 04. 2019 - 16. 04. 2019

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

Identifikátor

Adobe produkty viacero zraniteľností

Popis

Spoločnosť Adobe vydala aktualizácie na svoje produkty Acrobat, Acrobat Reader a Flash Player, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.04.2019

CVE

CVE-2019-7061, CVE-2019-7088, CVE-2019-7096, CVE-2019-7097, CVE-2019-7098, CVE-2019-7099, CVE-2019-7100, CVE-2019-7101, CVE-2019-7102, CVE-2019-7103, CVE-2019-7104, CVE-2019-7105, CVE-2019-7106, CVE-2019-7107, CVE-2019-7108, CVE-2019-7109, CVE-2019-7110, CVE-2019-7111, CVE-2019-7112, CVE-2019-7113, CVE-2019-7114, CVE-2019-7115, CVE-2019-7116, CVE-2019-7117, CVE-2019-7118, CVE-2019-7119, CVE-2019-7120, CVE-2019-7121, CVE-2019-7122, CVE-2019-7123, CVE-2019-7124, CVE-2019-7127, CVE-2019-7128, CVE-2019-7129, CVE-2019-7130, CVE-2019-7132, CVE-2019-7133, CVE-2019-7134, CVE-2019-7135, CVE-2019-7136, CVE-2019-7137, CVE-2019-7138

IOC

-

Zasiahnuté systémy

Acrobat DC staršie ako 2019.010.20099
Acrobat Reader DC staršie ako 2019.010.20099
Acrobat 2017 staršie ako 2017.011.30138
Acrobat Reader DC 2017 staršie ako 2017.011.30138
Acrobat DC Classic 2015 staršie ako 2015.006.30493
Acrobat Reader DC staršie ako 2015.006.30493
Adobe Flash Player verzie staršie ako 32.0.0.171

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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.

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:
01380/2019/TS/OKB-114

Zdroje
https://helpx.adobe.com/security/products/acrobat/apsb19-17.html
https://helpx.adobe.com/security/products/flash-player/apsb19-19.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/159246
https://exchange.xforce.ibmcloud.com/vulnerabilities/159252
https://exchange.xforce.ibmcloud.com/vulnerabilities/159253
https://exchange.xforce.ibmcloud.com/vulnerabilities/159254
https://exchange.xforce.ibmcloud.com/vulnerabilities/159255
https://exchange.xforce.ibmcloud.com/vulnerabilities/159245

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

Identifikátor

Adobe Shockwave Player viacero zraniteľností

Popis

Spoločnosť Adobe vydala aktualizáciu na svoj produkt Adobe Shockwave Player, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.04.2019

CVE

CVE-2019-7098, CVE-2019-7099, CVE-2019-7100, CVE-2019-7101, CVE-2019-7102, CVE-2019-7103, CVE-2019-7104

IOC

-

Zasiahnuté systémy

Adobe Shockwave Player verzie staršie ako 12.3.5.205

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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://helpx.adobe.com/security/products/shockwave/apsb19-20.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/159232
https://exchange.xforce.ibmcloud.com/vulnerabilities/159234
https://exchange.xforce.ibmcloud.com/vulnerabilities/159235
https://exchange.xforce.ibmcloud.com/vulnerabilities/159236
https://exchange.xforce.ibmcloud.com/vulnerabilities/159237
https://exchange.xforce.ibmcloud.com/vulnerabilities/159238
https://exchange.xforce.ibmcloud.com/vulnerabilities/159239

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Rockwell Automation Stratix a ArmorStratix zraniteľnosti

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje produkty Stratix a ArmorStratix, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

04.04.2019

CVE

CVE-2018-0466, CVE-2018-0467, CVE-2018-0470, CVE-2018-0472, CVE-2018-0473, CVE-2018-15373, CVE-2018-15377

IOC

-

Zasiahnuté systémy

Rockwell Automation Allen-Bradley Stratix 5400, 5410. 5700, 5950, 8000 verzie staršie ako 15.2(6)E2a
Rockwell Automation Allen-Bradley Stratix 8300 verzie staršie ako 15.2(4)EA7
Rockwell Automation Allen-Bradley ArmorStratix 5700

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Ak nepoužívate IPsec, odporúčame ho v nastaveniach zariadení Stratix 5950 vypnúť.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-094-02
https://ics-cert.us-cert.gov/advisories/ICSA-19-094-03
https://ics-cert.us-cert.gov/advisories/ICSA-19-094-04

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

Identifikátor

FTPShell Server viacero zraniteľností

Popis

Bezpečnostní výskumníci informovali o zraniteľnostiach v produkte FTPShell.
Bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.04.2019

CVE

IOC

-

Zasiahnuté systémy

FTPShell Server 6.83

Následky

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

Odporúčania

Na zraniteľnosť momentálne neexistuje bezpečnostná záplata.
Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Ak je to možné, oddeľte FTPShell Server od verejného internetu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/159328
https://exchange.xforce.ibmcloud.com/vulnerabilities/159326

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

Identifikátor

WPA3 hostapd a wpa_supplicant viacero zraniteľností

Popis

Bezpečnostní výskumníci objavili viacero zraniteľností v dizajne protokolu WPA3 a implementacií hostapd a wpa_supplicant.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.04.2019

CVE

CVE-2019-9494, CVE-2019-9495, CVE-2019-9496, CVE-2019-9497, CVE-2019-9498, CVE-2019-9499

IOC

-

Zasiahnuté systémy

wpa_supplicant a hostapd verzie staršie ako 2.8
Kompletný zoznam zasiahnutých systémov nájdete v časti Zdroje.

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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.kb.cert.org/vuls/id/871675/
https://securityaffairs.co/wordpress/83653/hacking/wpa3-security-flaws.html

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

Identifikátor

Wireshark viacero zraniteľností

Popis

Vývojári nástroja na sieťovú analýzu Wireshark vydali aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.04.2019

CVE

CVE-2019-10895, CVE-2019-10896, CVE-2019-10897, CVE-2019-10898, CVE-2019-10899, CVE-2019-10900, CVE-2019-10901

IOC

-

Zasiahnuté systémy

Wireshark verzie staršie ako 3.0.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.wireshark.org/docs/relnotes/
https://tools.cisco.com/security/center/viewAlert.x?alertId=59970
https://tools.cisco.com/security/center/viewAlert.x?alertId=59971
https://tools.cisco.com/security/center/viewAlert.x?alertId=59972
https://tools.cisco.com/security/center/viewAlert.x?alertId=59973
https://tools.cisco.com/security/center/viewAlert.x?alertId=59974
https://tools.cisco.com/security/center/viewAlert.x?alertId=59975
https://tools.cisco.com/security/center/viewAlert.x?alertId=59976