BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 05. 2019 - 21. 05. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe Flash Player zraniteľnosť	Vysoká	**8.8**
02.	Apple produkty viacero zraniteľností	Vysoká	**8.8**
03.	Adobe Acrobat a Reader zraniteľnosti	Vysoká	**8.8**
04.	Samba zraniteľnosť	Vysoká	**7.5**
05.	Omron zraniteľnosť	Vysoká	**7.3**
06.	Wacom zraniteľnosti	Vysoká	**7.1**

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-140

BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 05. 2019 - 21. 05. 2019

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

Identifikátor

Adobe Flash Player zraniteľnosť

Popis

Spoločnosť Adobe vydala aktualizáciu na svoj produkt Flash Player, ktorá opravuje bezpečnostnú zraniteľnosť.
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

14.05.2019

CVE

CVE-2019-7837

Zasiahnuté systémy

Adobe Flash Player verzie staršie ako 32.0.0.192

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, súbory 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://helpx.adobe.com/security/products/flash-player/apsb19-26.html
https://access.redhat.com/security/cve/cve-2019-7837
https://www.cisecurity.org/advisory/a-vulnerability-in-adobe-flash-could-allow-for-arbitrary-code-execution-apsb19-26_2019-054/

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-140

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

Identifikátor

Apple produkty viacero zraniteľností

Popis

Spoločnosť Apple vydala aktualizácie na svoje produkty watchOS, Apple TV Software, tvOS, iOS a macOS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

13.05.2019

CVE

CVE-2018-20346, CVE-2018-20505, CVE-2018-20506, CVE-2018-4452, CVE-2018-4467, CVE-2019-6200, CVE-2019-6202, CVE-2019-6205, CVE-2019-6206, CVE-2019-6208, CVE-2019-6209, CVE-2019-6210, CVE-2019-6211, CVE-2019-6212, CVE-2019-6213, CVE-2019-6214, CVE-2019-6215, CVE-2019-6216, CVE-2019-6217, CVE-2019-6218, CVE-2019-6219, CVE-2019-6220, CVE-2019-6221, CVE-2019-6224, CVE-2019-6225, CVE-2019-6226, CVE-2019-6227, CVE-2019-6228, CVE-2019-6229, CVE-2019-6230, CVE-2019-6231, CVE-2019-6233, CVE-2019-6234, CVE-2019-6235

Zasiahnuté systémy

watchOS verzie staršie ako 5.2.1
Safari verzie staršie ako 12.1.1
Apple TV Software 7.3
tvOS verzie staršie ako 12.3
iOS verzie staršie ako 12.3
macOS Mojave 10.14.5, macOS Sierra 10.12.6, macOS High Sierra 10.13.6

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame bezodkladne 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://support.apple.com/en-us/HT210118 https://support.apple.com/en-us/HT210119 https://support.apple.com/en-us/HT210120 https://support.apple.com/en-us/HT210121 https://support.apple.com/en-us/HT210122 https://support.apple.com/en-us/HT210123 https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2019-052/

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

Identifikátor

Adobe Acrobat a Reader zraniteľnosti

Popis

Spoločnosť Adobe vydala aktualizácie na svoje produkty Acrobat a Reader, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie 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

14.05.2019

CVE

CVE-2019-7140, CVE-2019-7141, CVE-2019-7142, CVE-2019-7143, CVE-2019-7144, CVE-2019-7145,
CVE-2019-7758, CVE-2019-7759, CVE-2019-7760, CVE-2019-7761, CVE-2019-7762, CVE-2019-7763,
CVE-2019-7764, CVE-2019-7765, CVE-2019-7766, CVE-2019-7767, CVE-2019-7768, CVE-2019-7769,
CVE-2019-7770, CVE-2019-7771, CVE-2019-7772, CVE-2019-7773, CVE-2019-7774, CVE-2019-7775,
CVE-2019-7776, CVE-2019-7777, CVE-2019-7778, CVE-2019-7779, CVE-2019-7780, CVE-2019-7781,
CVE-2019-7782, CVE-2019-7783, CVE-2019-7784, CVE-2019-7785, CVE-2019-7786, CVE-2019-7787,
CVE-2019-7788, CVE-2019-7789, CVE-2019-7790, CVE-2019-7791, CVE-2019-7792, CVE-2019-7793,
CVE-2019-7794, CVE-2019-7796, CVE-2019-7797, CVE-2019-7798, CVE-2019-7799, CVE-2019-7800,
CVE-2019-7801, CVE-2019-7802, CVE-2019-7803, CVE-2019-7804, CVE-2019-7805, CVE-2019-7806,
CVE-2019-7807, CVE-2019-7808, CVE-2019-7809, CVE-2019-7810, CVE-2019-7811, CVE-2019-7812,
CVE-2019-7813, CVE-2019-7814, CVE-2019-7817, CVE-2019-7818, CVE-2019-7820, CVE-2019-7821,
CVE-2019-7822, CVE-2019-7823, CVE-2019-7824, CVE-2019-7825, CVE-2019-7826, CVE-2019-7827,
CVE-2019-7828, CVE-2019-7829, CVE-2019-7830, CVE-2019-7831, CVE-2019-7832, CVE-2019-7833,
CVE-2019-7834, CVE-2019-7835, CVE-2019-7836

Zasiahnuté systémy

Adobe Acrobat a Reader verzie staršie ako 2019.012.20034, 2017.011.30142 a 2015.006.30497

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, súbory 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://helpx.adobe.com/security/products/acrobat/apsb19-18.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-acrobat-and-reader-could-allow-for-arbitrary-code-execution-apsb19-18_2019-055/

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

Identifikátor

Samba zraniteľnosť

Popis

Vývojári produktu Samba vydali aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

14.05.2019

CVE

CVE-2018-16860

Zasiahnuté systémy

Samba verzie staršie ako 4.10.3

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.samba.org/samba/history/samba-4.10.3.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=60197

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

Identifikátor

Omron zraniteľnosť

Popis

Spoločnosť Omron vydala aktualizáciu na svoj produkt Network Configurator, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.05.2019

CVE

CVE-2019-10971

Zasiahnuté systémy

Network Configurator pre DeviceNet Safety verzie staršie 3.41

Následky

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

Odporúčania

Na zraniteľnosť momentálne neexistuje bezpečnostná záplata.
Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-19-134-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Wacom zraniteľnosti

Popis

Spoločnosť Wacom vydala bezpečnostnú aktualizáciu na svoj produkt Wacom driver, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

16.05.2019

CVE

CVE-2019-5012, CVE-2019-5013

Zasiahnuté systémy

Wacom driver verzie staršie ako 6.3.34

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0760
https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0761
https://www.wacom.com/en/support/product-support/drivers