OBSAH BEZPEČNOSTNÉHO BULLETINU

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

Identifikátor

Adobe Acrobat and Reader Multiple Arbitrary Code Execution Vulnerabilities

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produktoch Adobe Acrobat a Adobe Acrobat Reader.
Najvážnejšiu bezpečnostnú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného PDF súboru mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ostatné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

19.09.2018

CVE

CVE-2018-12775, CVE-2018-12778, CVE-2018-12801, CVE-2018-12840, CVE-2018-12848, CVE-2018-12849, CVE-2018-12850

Zasiahnuté systémy

Acrobat DC, Acrobat Reader DC verzie 2018.011.20058 a staršie
Acrobat 2017, Acrobat Reader 2017 verzie 2017.011.30099 a staršie
Acrobat DC, Acrobat Reader DC verzie 2015.006.30448 a staršie

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/acrobat/apsb18-34.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-acrobat-and-reader-could-allow-for-arbitrary-code-execution-apsb18-34_2018-103/

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

Identifikátor

Apple macOS Mojave Security Updates

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoj operačný systém macOS Mojave 10.14, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a vykonať škodlivý kód na zasiahnutom systéme.
Ďalšia bezpečnostná zraniteľnosť v Bluetooth komponente je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému autentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

24.09.2018

CVE

CVE-2018-5383, CVE-2018-4324, CVE-2018-4353, CVE-2018-4321, CVE-2018-4333, CVE-2018-4336, CVE-2018-4344, CVE-2016-1777

Zasiahnuté systémy

macOS Mojave 10.14

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT209139

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

Identifikátor

Cisco Webex Network Recording Player Remote Code Execution Vulnerabilities

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty Cisco Webex, ktoré opravujú viacero bezpečnostných zraniteľností v komponente Cisco Webex Network Recording Player.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia upravených .arf súborov vykonať škodlivý kód a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.09.2018

CVE

CVE-2018-15414, CVE-2018-15421, CVE-2018-15422

Zasiahnuté systémy

Cisco Webex Meetings Suite (WBS32) - Webex Network Recording Player verzie staršie ako WBS32.15.10
Cisco Webex Meetings Suite (WBS33) - Webex Network Recording Player verzie staršie ako WBS33.3
Cisco Webex Meetings Online - Webex Network Recording Player verzie staršie ako 1.3.37
Cisco Webex Meetings Server - Webex Network Recording Player verzie staršie ako 3.0MR2

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180919-webex
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-webex-network-recording-player-for-advanced-recording-format-files-could-allow-for-arbitrary-code-execution_2018-104/

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

Identifikátor
Tec4Data SmartCooler Vulnerability

Popis
Spoločnosť Tec4Data vydala bezpečnostnú aktualizáciu na svoj produkt SmartCooler, ktorá opravuje bezpečnostnú zraniteľnosť v bezpečnostných nastaveniach. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému útočníkovi vykonať neautorizovaný príkaz na reštart systému a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania
20.09.2018

CVE
CVE-2018-14796

Zasiahnuté systémy
SmartCooler verzie firmvéru staršie ako 180806

Následky
Zneprístupnenie služby

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje
https://ics-cert.us-cert.gov/advisories/ICSA-18-263-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Windows JET Vulnerability

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v komponente JET Database Engine v operačných systémoch Microsoft Windows.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému útočníkovi pomocou podvrhnutia upravených Jet súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

20.09.2018

CVE

-

Zasiahnuté systémy

Operačné systémy Microsoft Windows

Následky

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

Odporúčania

Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky. Odporúčame dôsledne dodržiavať princíp najnižšieho privilégia a pokiaľ to nie je nevyhnutné, nespúšťať aplikácie s administrátorskými oprávneniami.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-18-1075/
https://www.cisecurity.org/advisory/a-vulnerability-in-microsoft-windows-jet-database-engine-could-allow-for-remote-code-execution_2018-105/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.3
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WECON PLC Editor Vulnerability

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v produkte WECON PLC Editor.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému útočníkovi pomocou podvrhnutia upravených súborov vykonať škodlivý kód v kontexte bežiaceho procesu.

Dátum prvého zverejnenia varovania

18.09.2018

CVE

CVE-2018-14792

Zasiahnuté systémy

WECON PLC Editor verzia 1.3.3U

Následky

Vykonanie škodlivého kódu

Odporúčania

Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-261-01