NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 09. 08. 2017 – 15. 08. 2017

No: B20170815-01V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Adobe Flash Player Security Bypass and Type Confusion Vulnerability

Popis

Spoločnosť Adobe vydala aktualizácie zabezpečenia pre program Adobe Flash Player pre operačné systémy Windows, Macintosh, Linux a Chrome OS. Tieto aktualizácie sa zaoberajú zraniteľnosťou, ktorá by mohla viesť k vykonaniu škodlivého kódu a zraniteľnosťou pri ktorej je možné obísť zabezpečenie, čo by mohlo viesť k úniku informácií.

CVE

CVE-2017-3085, CVE-2017-3106

Adobe bulletin ID

APSB17-23

Zasiahnuté systémy

Adobe Flash Player Desktop Runtime – verzia 26.0.0.137 a skoršie
Adobe Flash Player pre Google Chrome – verzia 26.0.0.137 a skoršie
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 - verzia 26.0.0.137 a skoršie

Následky

Neoprávnené spustenie škodlivého kódu, únik informácií

Odporúčania

Spoločnosť Adobe na vyššie uvedené zraniteľnosti vydala aktualizácie, preto odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://helpx.adobe.com/security/products/flash-player/apsb17-23.html

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 09. 08. 2017 – 15. 08. 2017

No: B20170815-02V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Adobe Acrobat and Reader important updates

Popis

Spoločnosť Adobe vydala aktualizácie zabezpečenia pre programy Adobe Acrobat a Reader pre systémy Windows a Macintosh. Tieto aktualizácie sa týkajú zraniteľných miest označených ako kritické a dôležité, ktoré by potenciálne umožnili útočníkovi prevziať kontrolu nad postihnutým systémom.

CVE

Zoznam všetkých CVE: https://helpx.adobe.com/security/products/acrobat/apsb17-24.html

Adobe bulletin ID

APSB17-24

Zasiahnuté systémy

Acrobat DC (Continuous Track)
Acrobat Reader DC (Continuous Track)
Acrobat 2017
Acrobat Reader 2017
Acrobat DC (Classic Track)
Acrobat Reader DC (Classic Track)
Acrobat XI
Reader XI

Následky

Neoprávnené spustenie škodlivého kódu, únik informácií

Odporúčania

Spoločnosť Adobe vydala komplexnú aktualizáciu vyššie uvedených produktov, preto odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://helpx.adobe.com/security/products/acrobat/apsb17-24.html

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 09. 08. 2017 – 15. 08. 2017

No: B20170815-03V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Adobe Experience Manager important updates

Popis

Spoločnosť Adobe vydala aktualizácie zabezpečenia aplikácie Adobe Experience Manager. Tieto aktualizácie vyriešia zraniteľnosť overovania typu súboru a zraniteľnosť možnosti úniku informácií.

CVE

CVE-2017-3107, CVE-2017-3108, CVE-2017-3110

Adobe bulletin ID

APSB17-26

Zasiahnuté systémy

Adobe Experience Manager – verzie 6.0, 6.1, 6.2, 6.3

Následky

Neoprávnené spustenie škodlivého kódu, únik informácií

Odporúčania

Spoločnosť Adobe vydala komplexnú aktualizáciu vyššie uvedeného produktu, preto odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://helpx.adobe.com/security/products/experience-manager/apsb17-26.html

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 09. 08. 2017 – 15. 08. 2017

No: B20170815-04V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Adobe Digital Editions important updates

Popis

Spoločnosť Adobe vydala aktualizáciu zabezpečenia pre aplikácie Adobe Digital Editions pre systémy Windows, Macintosh, iOS a Android. Táto aktualizácia rieši zraniteľnosť buffer overflow, ktorá by mohla viesť k spusteniu škodlivého kódu, sedem zraniteľností poškodenia pamäte, ktoré by mohli viesť k úniku adries pamäte a spracovaniu externej entity XML, ktorá by mohla viesť k úniku informácií.

CVE

CVE-2017-11274, CVE-2017-3091, CVE-2017-11275, CVE-2017-11276, CVE-2017-11277, CVE-2017-11278, CVE-2017-11279, CVE-2017-11280, CVE-2017-11272

Adobe bulletin ID

APSB17-27

Zasiahnuté systémy

Adobe Digital Editions – verzia 4.5.6

Následky

Neoprávnené spustenie škodlivého kódu, únik informácií

Odporúčania

Spoločnosť Adobe vydala komplexnú aktualizáciu vyššie uvedeného produktu, preto odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://helpx.adobe.com/security/products/Digital-Editions/apsb17-27.html

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 09. 08. 2017 – 15. 08. 2017

No: B20170815-05V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Junos OS: Integer signedness error in GD Graphics Library

Popis

Libgd je open-source obrazová knižnica, ktorá je súčasťou PHP verzie 4.3 a vyššie. Celá zraniteľnosť podpisu existuje v systéme libgd 2.1.1, čo môže viesť k buffer overflow pri spracovaní komprimovaných dát gd2.
Juniper SIRT si nie je vedomý žiadneho nebezpečného zneužitia tejto zraniteľnosti.

CVE

CVE-2016-3074

Zasiahnuté systémy

Junos OS - verzie 12.1X46, 12.3X48, 15.1X49, 14.2, 15.1, 15.1X53, 16.1, 16.2

Následky

Neoprávnené spustenie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Spoločnosť Jupiter vydala komplexnú aktualizáciu vyššie uvedeného produktu, preto odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10798&cat=SIRT_1&actp=LIST

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 09. 08. 2017 – 15. 08. 2017

No: B20170815-06V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Firefox ESR 52.3 important updates

Popis

Spoločnosť Firefox vydala dôležité aktualizácie na produkt Firefox ESR 52.3, ktoré riešia niektoré závažné zraniteľnosti.

CVE

CVE-2017-7798, CVE-2017-7800, CVE-2017-7801, CVE-2017-7809, CVE-2017-7784, CVE-2017-7802, CVE-2017-7785, CVE-2017-7786, CVE-2017-7753, CVE-2017-7787, CVE-2017-7807, CVE-2017-7792, CVE-2017-7804, CVE-2017-7791, CVE-2017-7782, CVE-2017-7803, CVE-2017-7779

Zasiahnuté systémy

Firefox ESR 52.3

Následky

Neoprávnené spustenie škodlivého kódu, Zneprístupnenie služby, Únik informácií

Odporúčania

Spoločnosť Firefox vydala komplexnú aktualizáciu vyššie uvedeného produktu, preto odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-19/

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SECURITY BULLETIN

Týždeň 09. 08. 2017 – 15. 08. 2017

No: B20170815-07V

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)				

Identifikátor

Firefox 55 important updates

Popis

Spoločnosť Firefox vydala dôležité aktualizácie na produkt Firefox 55, ktoré riešia niektoré závažné zraniteľnosti.

CVE

CVE-2017-7779, CVE-2017-7780, CVE-2017-7797, CVE-2017-7796, CVE-2017-7790, CVE-2017-7789, CVE-2017-7788, CVE-2017-7783, CVE-2017-7799, CVE-2017-7803, CVE-2017-7794, CVE-2017-7781, CVE-2017-7782, CVE-2017-7808, CVE-2017-7791, CVE-2017-7804, CVE-2017-7792, CVE-2017-7807, CVE-2017-7787, CVE-2017-7753, CVE-2017-7806, CVE-2017-7786, CVE-2017-7785, CVE-2017-7802, CVE-2017-7784, CVE-2017-7809, CVE-2017-7801, CVE-2017-7800, CVE-2017-7798

Zasiahnuté systémy

Firefox 55

Následky

Neoprávnené spustenie škodlivého kódu, Zneprístupnenie služby, Únik informácií

Odporúčania

Spoločnosť Firefox vydala komplexnú aktualizáciu vyššie uvedeného produktu, preto odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-18/