SECURITY BULLETIN

Týždeň 11. 10. 2017 – 17. 10. 2017

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☒ **Kritická**	**CVSS skóre: 10**
Klasifikácia	☒ **TLP (WHITE)**	☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**	
Kód sektora (dopad)					

Identifikátor

Oracle Critical Patch Update Advisory - October 2017

Popis

Spoločnosť Oracle vydala Critical Patch Update (CPU), balík opráv pre viaceré zraniteľnosti ich produktov. Októbrový CPU obsahuje aj opravy kritických zranietľností na produkty spoločnosti Oracle. Celkovo obsahuje 252 opráv zraniteľností v rôznych produktoch.

Dátum prvého zverejnenia varovania

17. 10. 2017

CVE

Kompletný zoznam CVE nájdete na: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html v prílohe Critical Patch Update

Zasiahnuté systémy

Kompletný zoznam zasiahnutých produktov nájdete na: http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html v časti „Affected products and Components“

Následky

Následky podľa typu zraniteľnosti v Critical Patch Update

Odporúčania

Spoločnosť Oracle vydala aktualizácie na vyššie uvedené produkty, ktoré opravujú jednotlivé zraniteľnosti. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2858*

SK-CERT
Naša značka:
06282/2017/SKB/OBPr-015

SECURITY BULLETIN

Týždeň 11. 10. 2017 – 17. 10. 2017

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

Identifikátor

Flash Player zero-day exploit in the wild

Popis

Spoločnosť Adobe vydala aktualizáciu pre Flash Player, odstraňujúcu zero-day zraniteľnosť typu vzdialené vykonanie škodlivého kódu.
Výskumníci z Kaspersky Lab zistili prepojenie tejto zraniteľnosti s FinSpy malvérom, ktorý bol v zraniteľných zariadeniach inštalovaný práve cez túto zero-day zraniteľnosť. Išlo o malvér, ktorý zariadenie pripojil na Command and Control server a následne vydával príkazy pre zariadenie alebo exfiltroval dáta z dotknutého zariadenia.

Dátum prvého zverejnenia varovania

16. 10. 2017

CVE

CVE-2017-11292

Vendor ID (Adobe Bulletin ID)

APSB17-32

Zasiahnuté systémy

Adobe Flash Player Desktop Runtime vo verzii 27.0.0.159 pre Windows a Macintosh
Adobe Flash Player for Google Chrome vo verzii 27.0.0.159 pre Windows, Macintosh, Linux a Chrome OS
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 vo verzii 27.0.0.130 pre Windows 10 a 8.1
Adobe Flash Player for Microsoft Edge and Internet Explorer 11 vo verzii 27.0.0.130 pre Windows 10 a 8.1

Následky

Vzdialené vykonanie kódu

Odporúčania

Spoločnosť Adobe vydala aktualizácie na vyššie uvedené produkty, ktoré riešia túto zraniteľnosť. Odporúčame bezodkladne tieto produkty aktualizovať.

Zdroje

https://helpx.adobe.com/security/products/flash-player/apsb17-32.html
https://www.helpnetsecurity.com/2017/10/17/emergency-fix-flash-player-zero-day/

SECURITY BULLETIN

Týždeň 11. 10. 2017 – 17. 10. 2017

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

Identifikátor

Security vulnerabilities fixed in Thunderbird 52.4

Popis

Spoločnosť Mozilla vydala aktualizáciu produktu Thunderbird 52.4, ktorá rieši niekoľko dôležitých zranitešností.

Dátum prvého zverejnenia varovania

09. 10. 2017

CVE

CVE-2017-7810, CVE-2017-7793, CVE-2017-7818, CVE-2017-7819, CVE-2017-7824, CVE-2017-7805, CVE-2017-7814, CVE-2017-7825, CVE-2017-7823,

Zasiahnuté systémy

Mozilla Thunderbird 52.4

Následky

Neoprávnené vykonanie škodlivého kódu, neoprávnený prístup k informáciám

Odporúčania

Spoločnosť Mozilla vydala aktualizácie na vyššie uvedený produkt, ktoré opravujú jednotlivé zraniteľnosti. Odporúčame bezodkladne tento produkt aktualizovať.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-23/