# BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 01. 2018 – 09. 01. 2018

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Číslo | Identifikátor | Dôležitosť | CVSS Score |
|---|---|---|---|
| 1 | Mozilla Releases Security Update | Vysoká | 8.4 |
| 2 | Multiple vulnerabilities in GIMP | Vysoká | 7.8 |
| 3 | XSRF/CSRF vulnerability in phpMyAdmin | Vysoká | 7.1 |
| 4 | Android Security Bulletin | Vysoká | 7.1 |
| 5 | iJoomla com_adagency 6.0.9 - SQL Injection Vulnerabilities | Vysoká | 7.1 |
| 6 | WebKitGTK+ vulnerabilities | Stredná | 6.8 |
| 7 | Memory Corruption Vulnerabilities in Microsoft browsers | Stredná | 6.7 |
| 8 | Linux Kernel Extended BPF multiple security vulnerabilities | Stredná | 6.3 |
| 9 | vRealize Operations multiple security vulnerabilities | Stredná | 5.3 |

**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-043

# BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 01. 2017 – 09. 01. 2017

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

## Identifikátor

Mozilla Releases Security Update

## Popis

Spoločnosť Mozilla vydala aktualizáciu svojho internetového prehliadača Mozilla Firefox, ktorá minimalizuje dopady bezpečnostných zraniteľností v architektúre CPU. Bezpečnostné útoky známe pod označením Meltdown a Spectre umožňujú vzdialenému útočníkovi prostredníctvom funkcií *performance.now()* a *SharedArrayBuffer* získať prístup k citlivým dátam v relácii internetového prehliadača.
Bezpečnostná aktualizácia deaktivuje funkciu *SharedArrayBuffer* a znižuje časovú presnosť funkcie *performance.now()* z 5µs na 20µs.

## Dátum prvého zverejnenia varovania

04.01.2018

## CVE

CVE-2017-5753, CVE-2017-5715, CVE-2017-5754

## Zasiahnuté systémy

Mozilla Firefox verzie nižšie ako 57.0.4

## Následky

Útočník môže zneužitím uvedených zraniteľností získať prístup k citlivým informáciám používateľa takým spôsobom, že napríklad infikovaním webovej stránky, ktorá je otvorená na jednom tabe môže získať prístup k informáciám z druhého otvoreného tabu v tom istom okne prehliadača. Takisto môže získať prístup k bezpečnostným certifikátom alebo uloženým heslám.

## Odporúčania

Administrátorom a používateľom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/
https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/

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

## Identifikátor

Multiple vulnerabilities in GIMP

## Popis

Softvér GIMP verzie 2.8.22 obsahuje viacero zraniteľností založených na pretečení zásobníka:
- vo funkcii *load_image* v *plug-ins/common/file-gbr.c* v gbr parseri (spôsobené nesprávnym spracovaním UTF-8 dát)
- vo funkcii *fli_read_brun* v *plug-ins/file-fli/fli.c*
- vo funkcii *ReadImage* v *plug-ins/common/file-tga.c* (spôsobené nesprávnou hodnotu bit-per-pixel v rámci RGBA obrázka)
- vo funkcii *read_creator_block* v *plug-ins/common/file-psp.c*
- vo funkcii *xcf_load_stream* v *app/xcf/xcf.c* (spôsobené nesprávnym zakončením textového reťazca s verziou)
- vo funkcii *read_channel_data* v *plug-ins/common/file-psp.c*

Prostredníctvom uvedených zraniteľností by útočník mohol spôsobiť pretečenie zásobníka, vykonanie škodlivého kódu alebo odopretie služby.

## Dátum prvého zverejnenia varovania

20.12.2017 (posledná aktualizácia 04.01.2017)

## CVE

CVE-2017-17784, CVE-2017-17785, CVE-2017-17786, CVE-2017-17787, CVE-2017-17788, CVE-2017-17789

## Zasiahnuté systémy

GIMP 8.2.22

## Následky

Neoprávnené vykonanie kódu, Odopretie služieb

## Odporúčania

Používateľom odporúčame vykonať aktualizáciu uvedeného produktu.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/136546

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

## Identifikátor

XSRF/CSRF vulnerability in phpMyAdmin

## Popis

phpMyAdmin obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený útočník prostredníctvom Cross-site request forgery (CSRF) útoku mohol zneužiť na vykonanie neoprávnených zásahov do systému, ako je mazanie tabuliek a údajov prostredníctvom príkazov DROP alebo TRUNCATE.

## Dátum prvého zverejnenia varovania

20.12.2017 (aktualizované 03.01.2018)

## CVE

CVE-2017-1000499

## Zasiahnuté systémy

phpMyAdmin staršie ako verzia 4.7.7

## Následky

Neoprávnená zmena v systéme

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizácie uvedeného produktu.

## Zdroje

https://www.phpmyadmin.net/security/PMASA-2017-9/
https://thehackernews.com/2018/01/phpmyadmin-hack.html

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

## Identifikátor

Android Security Bulletin

## Popis

Spoločnosť Google vydala aktualizáciu svojho operačného systému Android, ktorá rieši viacero bezpečnostných zraniteľností. Najvážnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia škodlivých súborov vykonať škodlivý kód, získať citlivé informácie a spôsobiť odopretie služieb.

## Dátum prvého zverejnenia varovania

02.01.2018 (aktualizácia 05.01.2018)

## CVE

CVE-2013-4397, CVE-2017-0855, CVE-2017-0869, CVE-2017-11010, CVE-2017-11069, CVE-2017-13176, CVE-2017-13177, CVE-2017-13178, CVE-2017-13179, CVE-2017-13180, CVE-2017-13181, CVE-2017-13182, CVE-2017-13183, CVE-2017-13184, CVE-2017-13191, CVE-2017-13192, CVE-2017-13193, CVE-2017-13195, CVE-2017-13196, CVE-2017-13197, CVE-2017-13199, CVE-2017-13208, CVE-2017-13209, CVE-2017-13210, CVE-2017-13211, CVE-2017-13214, CVE-2017-13215, CVE-2017-13216, CVE-2017-13217, CVE-2017-13218, CVE-2017-13225, CVE-2017-14497, CVE-2017-14906, CVE-2017-14911, CVE-2017-14912, CVE-2017-14913, CVE-2017-14915, CVE-2017-15849

## Zasiahnuté systémy

Google Android

## Následky

Únik citlivých informácií, Odopretie služieb

## Odporúčania

Používateľom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://source.android.com/security/bulletin/2018-01-01
https://securitytracker.com/id/1040106

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

## Identifikátor

iJoomla com_adagency 6.0.9 - SQL Injection Vulnerabilities

## Popis

Bolo objavených viacero bezpečnostných zraniteľností v e-commerce rozšírení *Ad Agency* pre populárny redakčný systém Joomla!. Bezpečnostné zraniteľnosti nachádzajúce sa v parametroch *"advertiser_status"* a *"status_select"* v komponente *com_adagency* umožňujú vzdialenému útočníkovi prostredníctvom SQL injekcie vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

04.01.2018

## CVE

-

## Zasiahnuté systémy

Plugin com_adagency 6.0.9 pre Joomla!

## Následky

Vykonanie škodlivého kódu

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

## Zdroje

https://www.vulnerability-lab.com/get_content.php?id=1927

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

## Identifikátor

WebKitGTK+ vulnerabilities

## Popis

Boli vydané aktualizácie na linuxové distribúcie využívajúce *WebKitGTK+*. Bezpečnostné zraniteľnosti vo *WebKitGTK+* umožňujú vzdialenému útočníkovi pomocou podvrhnutého webového obsahu spôsobiť odopretie služieb a vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

28.12.2017 (aktualizované 03.01.2018)

## CVE

CVE-2017-13856, CVE-2017-13866, CVE-2017-13870, CVE-2017-7156

## Zasiahnuté systémy

Linuxové distribúcie využívajúce softvérové balíky libwebkit2gtk a libjavascriptcoregtk

## Následky

Vykonanie škodlivého kódu, odopretie služieb

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizácie uvedených produktov.

## Zdroje

https://usn.ubuntu.com/usn/usn-3514-1/
http://www.linuxsecurity.com/content/view/206082?rdf
http://www.linuxsecurity.com/content/view/209736?rdf

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.7 |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Memory Corruption Vulnerabilities in Microsoft browsers

## Popis

Webové prehliadače od spoločnosti Microsoft obsahujú zraniteľnosti, ktoré by vzdialený útočník mohol zneužiť na vykonanie ľubovoľného kódu v kontexte aktuálne prihláseného používateľa. V skriptovacom jadre zasiahnutých prehliadačov dochádza k nesprávnemu spracovaniu objektov v pamäti. Zneužitím zraniteľnosti útočník získava práva aktuálne prihláseného používateľa a ak sa jedná o administrátora, získava úplnú kontrolu nad systémom. Útočník následne môže vykonať inštaláciu programov, modifikovať dáta alebo vytvárať používateľské účty.

## Dátum prvého zverejnenia varovania

03.01.2018

## CVE

CVE-2018-0758, CVE-2018-0762, CVE-2018-0769, CVE-2018-0772, CVE-2018-0773, CVE-2018-0774, CVE-2018-0776, CVE-2018-0777, CVE-2018-0778

## Zasiahnuté systémy

Microsoft Internet Explorer 9, 10, 11
Microsoft Edge

## Následky

Neoprávnené vykonanie kódu

## Odporúčania

Administrátorom a používateľom dotknutých softwarov odporúčame vykonať aktualizáciu.

## Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0758
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0762
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0769
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0772
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0773
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0774
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0776
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0777
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0778

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

## Identifikátor

Linux Kernel Extended BPF multiple security vulnerabilities

## Popis

Linux Kernel obsahuje viacero bezpečnostných zraniteľností v prvku Extented Berkeley Packet Filter (eBPF). Zraniteľnosť v rámci funkcie *kernel/bpf/verifier.c* by útočník mohol zneužiť na vyvolanie pretečenia zásobníka, následné vykonanie ľubovoľného kódu a zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

08.01.2018

## CVE

CVE-2017-17862, CVE-2017-17863, CVE-2017-17864

## Zasiahnuté systémy

Linux Kernel

## Následky

Neoprávnený prístup k citlivým údajom, Eskalácia privilégií, Odopretie služby

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedených produktov.

## Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=56416
https://tools.cisco.com/security/center/viewAlert.x?alertId=56415
https://tools.cisco.com/security/center/viewAlert.x?alertId=56417

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 5.3** |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

vRealize Operations multiple security vulnerabilities

## Popis

Viaceré produkty spoločnosti VMware obsahujú novoobjavené bezpečnostné zraniteľnosti. Bezpečnostné zraniteľnosti vo funkciách *Cortado ThinPrint* a *Unity mode* umožňujú autentifikovanému, lokálnemu útočníkovi získať citlivé dáta, spôsobiť odopretie služieb a vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

04.01.2018

## CVE

CVE-2017-4945, CVE-2017-4946, CVE-2017-4948

## Zasiahnuté systémy

vRealize Operations for Horizon (V4H), vRealize Operations for Published Applications (V4PA), VMware Workstation Pro / Player (Workstation), VMware Fusion Pro / Fusion (Fusion),Horizon View Client for Windows

## Následky

Eskalácia privilégií, Únik citlivých informácií, Neoprávnená zmena v systéme

## Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedených produktov.

## Zdroje

https://www.vmware.com/us/security/advisories/VMSA-2018-0003.html
https://www.securitytracker.com/id/1040109