# BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 04. 2018 – 10. 04. 2018

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|---|---|---|---|
| **01.** | Pixel/Nexus Security Bulletin—April 2018 | Vysoká | **8.8** |
| **02.** | Ruby Multiple Vulnerabilities | Vysoká | **7.5** |
| **03.** | Multiple vulnerabilities in the IBM GSKit component of IBM Spectrum Protect Client | Vysoká | **7.4** |
| **04.** | Dell EMC Avamar Access Control Flaw in Installation Manager | Vysoká | **7.2** |
| **05.** | Trend Micro Security (Consumer) 2018 Multiple Vulnerabilities | Vysoká | **7.2** |
| **06.** | WolfCMS Multiple Vulnerabilities | Stredná | **6.8** |
| **07.** | Moodle Fixes Multiple Vulnerabilities | Stredná | **6.2** |
| **08.** | FreeBSD Multiple Vulnerabilities | Stredná | **6.2** |
| **09.** | Sophos Endpoint Protection Tamper Protection Bypass | Stredná | **6.2** |
| **10.** | GitLab Security Release | Stredná | **6.1** |

**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:
02049/2018/TS/OKB-031

# BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 04. 2018 – 10. 04. 2018

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

## Identifikátor

Pixel/Nexus Security Bulletin—April 2018

## Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na svoje zariadenia Pixel/Nexus, ktoré opravujú 41 rôznych bezpečnostných zraniteľností.
Najvážnejšími sú zraniteľnosti v Media framework, ktoré umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služieb.

## Dátum prvého zverejnenia varovania

02.04.2018

## CVE

CVE-2017-11075, CVE-2017-13294, CVE-2017-13295, CVE-2017-13296, CVE-2017-13297, CVE-2017-13298, CVE-2017-13299, CVE-2017-13300, CVE-2017-13301, CVE-2017-13302, CVE-2017-13303, CVE-2017-13304, CVE-2017-13305, CVE-2017-13306, CVE-2017-13307, CVE-2017-14880, CVE-2017-14890, CVE-2017-14894, CVE-2017-15115, CVE-2017-15836, CVE-2017-15837, CVE-2017-15853, CVE-2017-15855, CVE-2017-17449, CVE-2017-17712, CVE-2017-8269, CVE-2018-3567, CVE-2018-3568, CVE-2018-3584, CVE-2018-3596, CVE-2018-3598, CVE-2018-3599, CVE-2018-5820, CVE-2018-5821, CVE-2018-5822, CVE-2018-5823, CVE-2018-5824, CVE-2018-5825, CVE-2018-5826, CVE-2018-5827, CVE-2018-5828

## Zasiahnuté systémy

Google Pixel, Pixel XL, Pixel 2, Pixel 2 XL, Pixel C, Nexus 5X, Nexus 6P

## Následky

Zneprístupnenie služby, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

## Odporúčania

Administrátorom a používateľom zasiahnutých produktov odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://source.android.com/security/bulletin/pixel/2018-04-01

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

## Identifikátor

Ruby Multiple Vulnerabilities

## Popis

Vývojári programovacieho jazyka Ruby vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v komponente WEBrick umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom posielania veľkého množstva požiadaviek s dlhými HTTP hlavičkami spôsobiť zneprístupnenie služieb.

## Dátum prvého zverejnenia varovania

05.04.2018

## CVE

CVE-2018-6914, CVE-2018-8778, CVE-2018-8779, CVE-2018-78780, CVE-2018-1000077, CVE-2018-1000079, CVE-2017-17742

## Zasiahnuté systémy

Ruby verzie staršie ako 2.5.1

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

## Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=57327
https://tools.cisco.com/security/center/viewAlert.x?alertId=57429
https://tools.cisco.com/security/center/viewAlert.x?alertId=57405
https://tools.cisco.com/security/center/viewAlert.x?alertId=57403

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

## Identifikátor

Multiple vulnerabilities in the IBM GSKit component of IBM Spectrum Protect Client

## Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt BM Spectrum Protect Client, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov pri spracovávaní ICC požiadaviek a umožňuje vzdialenému neautentifikovanému útočníkovi získať prístup k citlivým údajom.

## Dátum prvého zverejnenia varovania

29.03.2018 (posledná aktualizácia 06.04.2018)

## CVE

CVE-2018-1426, CVE-2018-1427, CVE-2018-1428, CVE-2018-1447, CVE-2016-0702, CVE-2016-0705, CVE-2017-3732, CVE-2017-3736

## Zasiahnuté systémy

IBM Spectrum Protect Client verzie 8.1.0.0 až 8.1.4.0
IBM Spectrum Protect Client verzie 7.1.0.0 až 7.1.8.1
IBM Spectrum Protect Client verzie 6.4 a staršie

## Následky

Únik citlivých informácií, Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

## Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22014669

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.2** |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Dell EMC Avamar Access Control Flaw in Installation Manager

## Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoje produkty Dell EMC, ktorá opravuje bezpečnostnú zraniteľnosť v Local Download Service.
Bezpečnostná zraniteľnosť spočívajúca v nedostatočnej implementácií bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi neoprávnený prístup k citlivým údajom a zneprístupnenie služby.

## Dátum prvého zverejnenia varovania

05.04.2018

## CVE

CVE-2018-1217

## Zasiahnuté systémy

Dell EMC Avamar Server 7.3.1
Dell EMC Avamar Server 7.4.1
Dell EMC Avamar Server 7.5.0
Dell EMC Integrated Data Protection Appliance 2.0
Dell EMC Integrated Data Protection Appliance 2.1

## Následky

Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

## Zdroje

https://www.securitytracker.com/id/1040641
http://seclists.org/fulldisclosure/2018/Apr/14

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☒ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 7.2** |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Trend Micro Security (Consumer) 2018 Multiple Vulnerabilities

## Popis

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie na svoje Security produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému autentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

## Dátum prvého zverejnenia varovania

04.04.2018

## CVE

CVE-2018-6232, CVE-2018-6233, CVE-2018-6234, CVE-2018-6235

## Zasiahnuté systémy

Antivirus+ Security verzia 12 a staršie
Internet Security verzia 12 a staršie
Maximum Security verzia 12 a staršie
Premium Security verzia 12 a staršie

## Následky

Eskalácia privilégií

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

## Zdroje

https://esupport.trendmicro.com/en-us/home/pages/technical-support/1119591.aspx

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

## Identifikátor

WolfCMS Multiple Vulnerabilities

## Popis

Vývojári systému pre správu obsahu WolfCMS vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostné zraniteľnosti v autentifikačných mechanizmoch. Bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených požiadaviek pri útoku typu CSRF (Cross-Site Request Forgery) získať neoprávnený prístup do systému.

## Dátum prvého zverejnenia varovania

04.04.2018

## CVE

CVE-2018-8813, CVE-2018-8814

## Zasiahnuté systémy

WolfCMS verzie staršie ako 0.8.3.1

## Následky

Neoprávnený prístup do systému, Neoprávnená zmena v systéme

## Odporúčania

Odporúčame uistiť sa, či Vaše webové aplikácie nie sú založené na systéme pre správu obsahu WolfCMS v zraniteľných verziách. V prípade, že áno, zabezpečte aktualizáciu systému.

## Zdroje

https://docs.google.com/document/d/19X9j9lMVrH7VPhyMEdqidqgW4VBhXaFibuBDyiPxJjc/edit
https://docs.google.com/document/d/1rdl1yWDJkPuuOFb2sF07_c3twl5uMkH9a-OO2OmYMus/edit
https://nvd.nist.gov/vuln/detail/CVE-2018-8813
https://nvd.nist.gov/vuln/detail/CVE-2018-8814

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.2 |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Moodle Fixes Multiple Vulnerabilities

## Popis

Vývojári e-learningového systému Moodle vydali aktualizáciu svojho produktu, ktorá rieši viaceré bezpečnostné zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť sa nachádza v Paypal IPN callback skripte a umožňuje lokálnemu neautentifikovanému útočníkovi prostredníctvom daného skriptu zasielať nevyžiadané správy administrátorovi a spôsobiť zneprístupnenie služieb.

## Dátum prvého zverejnenia varovania

04.04.2018

## CVE

CVE-2018-1081, CVE-2018-1082

## Zasiahnuté systémy

Moodle verzie staršie ako 3.4.2, 3.3.5, 3.2.8 a 3.1.11

## Následky

Zneprístupnenie služby, Neoprávnený prístup do systému

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

## Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2018-1081
https://moodle.org/mod/forum/discuss.php?d=367939
https://nvd.nist.gov/vuln/detail/CVE-2018-1082
https://moodle.org/mod/forum/discuss.php?d=367938

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.2 |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

FreeBSD Multiple Vulnerabilities

## Popis

Vývojári operačného systému FreeBSD vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viaceré bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť v module IPSec umožňuje vzdialenému útočníkovi prostredníctvom zasielanie špeciálne upravených paketov spôsobiť zneprístupnenie služby.
Druhá bezpečnostná zraniteľnosť sa nachádza vo vt(4) ovládači a umožňuje lokálnemu útočníkovi prostredníctvom nahratia špeciálne upraveného fontu získať prístup k citlivým údajom v systémovej pamäti.

## Dátum prvého zverejnenia varovania

04.04.2018

## CVE

CVE-2018-6918, CVE-2018-6917

## Zasiahnuté systémy

Operačný systém FreeBSD

## Následky

Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

## Zdroje

https://www.freebsd.org/security/advisories/FreeBSD-SA-18%3A05.ipsec.asc
https://www.freebsd.org/security/advisories/FreeBSD-SA-18%3A04.vt.asc

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.2 |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Sophos Endpoint Protection Tamper Protection Bypass

## Popis

Spoločnosť Sophos vydala bezpečnostnú aktualizáciu na svoj produkt Sophos Endpoint Protection, ktorá opravuje bezpečnostnú zraniteľnosť v Tamper Protection funkcii. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním zabezpečenia kľúča databázy registrov a umožňuje vzdialenému útočníkovi vykonať škodlivý kód a deaktivovať zabezpečenie Enhanced Tamper Protection.

## Dátum prvého zverejnenia varovania

04.04.2018

## CVE

CVE-2018-4863

## Zasiahnuté systémy

Sophos Endpoint Protection v10.7 a staršie

## Následky

Neoprávnená zmena v systéme, Vykonanie škodlivého kódu

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

## Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/141220
http://seclists.org/fulldisclosure/2018/Apr/10

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre:** 6.1 |
| **Klasifikácia** | ☒ **Neutajované / TLP (WHITE)** | | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

GitLab Security Release

## Popis

Vývojári softvéru GitLab vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností spôsobených nedostatočným overovaním používateľských vstupov.
Bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia vlastného kódu získať prístup k citlivým informáciám.

## Dátum prvého zverejnenia varovania

04.04.2018

## CVE

CVE-2018-9244, CVE-2018-9243

## Zasiahnuté systémy

GitLab Community Edition (CE) a Enterprise Edition (EE) verzie staršie ako 10.6.3, 10.5.7, a 10.4.7

## Následky

Únik citlivých informácií

## Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

## Zdroje

https://about.gitlab.com/2018/04/04/security-release-gitlab-10-dot-6-dot-3-released/
https://nvd.nist.gov/vuln/detail/CVE-2018-9244
https://nvd.nist.gov/vuln/detail/CVE-2018-9243