# BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 12. 2017 – 12. 12. 2017

## OBSAH BEZPEČNOSTNÉHO BULLETINU

| Číslo | Identifikátor | Dôležitosť | CVSS Score |
|---|---|---|---|
| **1** | Apple Security Update macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan | Kritická | **9.8** |
| **2** | Stable Chanel update for Google Chrome | Vysoká | **8.8** |
| **3** | Red Hat Security Advisory RHSA-2017:3392 | Vysoká | **8.8** |
| **4** | Siemens Multiple Industrial Products Improper Input Validation Denial of Service Vulnerability | Vysoká | **7.5** |
| **5** | Linux kernel denial of service | Stredná | **6.1** |
| **6** | Synaptics Touchpad Driver Potential | Stredná | **6.1** |
| **7** | OpenSSL Security Advisory | Stredná | **5.9** |
| **8** | Mozilla Foundation Security Advisory 2017-29 | Stredná | **5.6** |

**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-034

# BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 12. 2017 – 12. 12. 2017

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☐ **Stredná** | ☐ **Vysoká** | ☒ **Kritická** | **CVSS skóre: 9.8** |
| **Klasifikácia** | ☒ **TLP (WHITE)** | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** | |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Apple Security Update macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan

## Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty macOS High Sierra , Sierra a El Capitan, ktoré riešia viacero zraniteľností v daných produktoch. Najvážnejšou zraniteľnosťou je kritická zraniteľosť v macOS High Sierra, ktorá spočívala v eskalácii privilégií, kedy mohol vzdialený útočník získať administrátorský prístup do zariadenia bez interakcie používateľa.
Túto kritickú zraniteľnosť SK-CERT notifikoval varovaním zo dňa 29. 11. 2017 pod číslom V20171129-01K.

## Dátum prvého zverejnenia varovania

06.12.2017

## CVE

CVE-2017-9798, CVE-2017-1000254, CVE-2017-13872, CVE-2017-13883, CVE-2017-13878, CVE-2017-13875, CVE-2017-13844, CVE-2017-13848, CVE-2017-13858, CVE-2017-13847, CVE-2017-13862, CVE-2017-13833, CVE-2017-13876, CVE-2017-13855, CVE-2017-13867, CVE-2017-13865, CVE-2017-13868, CVE-2017-13869, CVE-2017-13871, CVE-2017-13860, CVE-2017-3735, CVE-2017-13826

## Zasiahnuté systémy

macOS High Sierra, macOS Sierra, OS X El Capitan

## Následky

Eskalácia privilégií, Neoprávnené vykonanie kódu, Neoprávnený prístup do systému

## Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať štandardnú aktualizáciu zasiahnutých operačných systémov.

## Zdroje

https://support.apple.com/en-us/HT208331
https://tools.cisco.com/security/center/viewAlert.x?alertId=56174

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

## Identifikátor

Stable Chanel update for Google Chrome

## Popis

Spoločnosť Google vydala aktualizáciu na produkt Google Chrome, verzia 63.0.3239.84, ktorá obsahuje viacero opráv dôležitých zraniteľností.

## Dátum prvého zverejnenia varovania

06.12.2017

## CVE

CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15414, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15421, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427

## Zasiahnuté systémy

Google Chrome

## Následky

Neoprávnené vykonanie kódu, Neprístupnosť služby

## Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

## Zdroje

https://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop.html

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

## Identifikátor

Red Hat Security Advisory RHSA-2017:3392

## Popis

Spoločnosť Red Hat vydala bezpečnostnú aktualizáciu pre svoj produkt Red Hat Enterprise Linux, ktorá opravuje viacero zraniteľností v OpenJDK. Najzávažnejšie zraniteľnosti v RMI and Hotspot súčastiach OpenJDK umožňujú vzdialenému útočníkovi pomocou Java aplikácie či appletu obísť zabezpečenie Java sandbox a vykonať škodlivý kód.

## Dátum prvého zverejnenia varovania

06.12.2017

## CVE

CVE-2017-10193, CVE-2017-10198, CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

## Zasiahnuté systémy

Red Hat Enterprise Linux

## Následky

Neoprávnený prístup do systému, neoprávnené vykonanie kódu

## Odporúčania

Používateľom a administrátorom Red Hat Enterprise Linux odporúčame vykonať bezpečnostnú aktualizáciu.

## Zdroje

https://access.redhat.com/errata/RHSA-2017:3392

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

## Identifikátor

Siemens Multiple Industrial Products Improper Input Validation Denial of Service Vulnerability

## Popis

Bezpečnostná zraniteľnosť vo viacerých priemyselných produktoch Siemens umožňuje vzdialenému útočníkovi spôsobiť odopretie služieb.
Zraniteľnosť je spôsobená nesprávnym spracovaním určitých paketov danými zariadeniami. Útočník môže pomocou špeciálne vytvorených paketov posielaných na dané zariadenia cez UDP port 161 spôsobiť zlyhanie zariadenia a odopretie služby.
Ak nastane takáto situácia (zlyhanie zariadenia a následné odopretie služby), zariadenie nebude fungovať až do fyzického reštartu.

## Dátum prvého zverejnenia varovania

23.11.2017 (posledná aktualizácia 05.12.2017)

## CVE

CVE-2017-12741

## Zasiahnuté systémy

SIMATIC S7-200 Smart: Všetky verzie nižšie ako V2.03.01, SIMATIC S7-400 PN V6: Všetky verzie nižšie ako V6.0.6,
SIMATIC: S7-400 H V6, S7-400 PN/DP V7, S7-410 V8, S7-300, S7-1200, S7-1500, S7-1500 Software Controller, WinAC RTX 2010 incl. F – Všetky verzie
SIMATIC ET 200 Interface modules for PROFINET IO: ET 200AL, ET 200ecoPN, ET 200M, ET 200MP, ET 200pro, ET 200S, SIMATIC ET 200SP, - Všetky verzie
Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller, EK-ERTEC 200P – všetky verzie nižšie ako V4.5, EK-ERTEC 200 PN IO – všetky verzie
SIMOTION Firmware: SIMOTION D, SIMOTION C, SIMOTION P – všetky verzie nižšie ako V5.1 HF1
SINAMICS, SINUMERIK 840D sl, SIMATIC Compact Field Unit, PN/PN Coupler, SIMOCODE pro V PROFINET, SIRIUS Soft starter 3RW44 PN – všetky verzie

## Následky

Zneprístupnenie služby

## Odporúčania

Administrátorom odporúčame aktualizovať zasiahnuté systémy.

## Zdroje

https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-346262.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-17-339-01
https://tools.cisco.com/security/center/viewAlert.x?alertId=56129

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

## Identifikátor

Linux kernel denial of service

## Popis

Zistená zraniteľnosť v Linux Kernel 2.6.32 a novšom umožňuje vzdialenému útočníkovi priamy prístup na I/O port 0x80, pričom môže dôjsť k zahlteniu daného portu požiadavkami na zápis a následnému pádu systému.

## Dátum prvého zverejnenia varovania

01.12.2017, aktualizované 11.12.2017

## CVE

CVE-2017-1000407

## Zasiahnuté systémy

OS linux využívajúce Linux Kernel 2.6.32 a novšie

## Následky

Odopretie služby

## Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

## Zdroje

https://access.redhat.com/security/cve/cve-2017-1000407
https://www.spinics.net/lists/kvm/msg159809.html

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

## Identifikátor

Synaptics Touchpad Driver Potential

## Popis

Zistená zraniteľnosť v ovládači touchpadu Synaptics v notebookoch HP umožňuje lokálnemu útočníkovi zaznamenávať sekvenciu používateľských vstupov z klávesnice a ukladať ich do súboru na lokálnom disku.

## Dátum prvého zverejnenia varovania

07.11.2017, aktualizované 07.12.2017

## Vendor ID

PSR-2017-0137

## Zasiahnuté systémy

Notebooky HP, kompletný zoznam je na stránke:
https://support.hp.com/us-en/document/c05827409

## Následky

Únik citlivých informácií

## Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

## Zdroje

https://support.hp.com/us-en/document/c05827409
https://zwclose.github.io/HP-keylogger/

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 5.9** |
| **Klasifikácia** | ☒ **TLP (WHITE)** | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** | |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

OpenSSL Security Advisory

## Popis

Boli zistené zraniteľnosti v OpenSSL. Vzdialený útočník môže v určitých limitovaných prípadoch obísť šifrovanie aplikácie a získať citlivé informácie vďaka chybe v spôsobe, akým aplikácia spracúva chyby pri nadväzovaní šifrovaného spojenia.

## Dátum prvého zverejnenia varovania

07.12.2017

## CVE

CVE-2017-3737, CVE-2017-3738

## Zasiahnuté systémy

OpenSSL staršie ako verzia 1.0.2n

## Následky

Únik citlivých informácií

## Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

## Zdroje

https://securitytracker.com/id/1039978

| | | | | | |
|---|---|---|---|---|---|
| **Dôležitosť** | ☐ **Nízka** | ☒ **Stredná** | ☐ **Vysoká** | ☐ **Kritická** | **CVSS skóre: 5.6** |
| **Klasifikácia** | ☒ **TLP (WHITE)** | ☐ **Vyhradené** | ☐ **Dôverné** | ☐ **Tajné** | |
| **Kód sektora (dopad)** | | | | | |

## Identifikátor

Mozilla Foundation Security Advisory 2017-29

## Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v prehliadači Firefox 57. Vzdialený útočník môže zneužitím chyby v Direct 3D 9 spôsobiť pretečenie zásobníka a následný pád aplikácie.

## Dátum prvého zverejnenia varovania

06.12.2017

## CVE

CVE-2017-7845

## Zasiahnuté systémy

Mozilla Firefox starší ako verzia 57.0.2. a Firefox ESR starší ako verzia 52.5.2, zasiahnutá je iba platforma Windows

## Následky

Neprístupnosť služby

## Odporúčania

Používateľom a administrátorom odporúčame vykonať štandardnú aktualizáciu uvedeného produktu.

## Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2017-29/