BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 03. 2018 – 13. 03. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-018

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 03. 2018 – 13. 03. 2018

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

Identifikátor

Google Chrome Stable Channel Update for Desktop

Popis

Spoločnosť Google vydala aktualizáciu na produkt Google Chrome, verzia 65.0.3325.146, ktorá obsahuje opravy viacerých chýb a 30 bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený útočník mohol zneužiť na vykonanie škodlivého kódu v kontexte prehliadača, neoprávnený prístup k citlivým údajom alebo zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

06.03.2018

CVE

CVE-2018-6057, CVE-2018-6058, CVE-2018-6059, CVE-2018-6060, CVE-2018-6061, CVE-2018-6062, CVE-2018-6063, CVE-2018-6063, CVE-2018-6064, CVE-2018-6065, CVE-2018-6066, CVE-2018-6067, CVE-2018-6068, CVE-2018-6069, CVE-2018-6070, CVE-2018-6071, CVE-2018-6072, CVE-2018-6073, CVE-2018-6074, CVE-2018-6075, CVE-2018-6076, CVE-2018-6077, CVE-2018-6078, CVE-2018-6079, CVE-2018-6080, CVE-2018-6081, CVE-2018-6082, CVE-2018-6083, CVE-2017-11215, CVE-2017-11225

Zasiahnuté systémy

Google Chrome

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti údajov

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať aktualizáciu uvedeného produktu.

Zdroje

https://chromereleases.googleblog.com/2018/03/stable-channel-update-for-desktop.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

mbed TLS Multiple Remote Code Execution Vulnerabilities

Popis

Knižnica mbed TLS obsahuje viacero bezpečnostných zraniteľností, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.
Prvá zraniteľnosť spočíva v nesprávnom overovaní RSASSA-PSS (RSA Probabilistic Signature Scheme) podpisov a útočník by ju prostredníctvom podvrhnutia špeciálne vytvorenej reťaze certifikátov mohol zneužiť na vyvolanie pretečenia zásobníka.
Druhá zraniteľnosť spočíva v nesprávnom spracovaní paketov v systémoch využívajúcich HMAC (Hash-based Message Authentication Code) pracujúci v prevádzkovom režime CBC (Cipher Block Chain) a útočník by ju mohol zneužiť poškodenie vybraných byte-ov zásobníka.

Dátum prvého zverejnenia varovania

01.02.2018 (posledná aktualizácia 12.03.2018)

CVE

CVE-2018-0487, CVE-2018-0488

Zasiahnuté systémy

mbed TLS verzie 1.3.8 až 1.3.21
mbed TLS verzie 2.1.0 až 2.1.9
mbed TLS verzie 2.4.0, 2.4.2

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tls.mbed.org/tech-updates/security-advisories/mbedtls-security-advisory-2018-01
https://tools.cisco.com/security/center/viewAlert.x?alertId=57164
https://tools.cisco.com/security/center/viewAlert.x?alertId=57163

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

Identifikátor

Multiple Vulnerabilities in Hirschmann Automation and Control Switches

Popis

Sieťové komponenty (switche) spoločnosti Hirschmann Automation and Control obsahujú viacero zraniteľností, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na obídenie mechanizmov autentifikácie a neoprávnený prístup k citlivým údajom.
Zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných a autentifikačných mechanizmov, ktoré umožňujú realizáciu brute-force útoku na manažmentové rozhranie zariadení alebo Man-In-The-Middle útoku.

Dátum prvého zverejnenia varovania

06.03.2018 (posledná aktualizácia 10.03.2018)

CVE

CVE-2018-5461, CVE-2018-5465, CVE-2018-5467, CVE-2018-5469, CVE-2018-5471

Zasiahnuté systémy

Classic Platform Switche: RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS
všetky verzie

Následky

Neoprávnený prístup do systému, Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Spoločnosť Hirschmann odporúča limitovať prístup k manažmentovému rozhraniu zasiahnutých produktov nasledujúcim spôsobom:
- obmedziť prístup k manažmentovému rozhraniu len na protokoly HTTPS alebo SSH,
- limitovať prístup k zariadeniam na základe IP adresy prostredníctvom funkcie "Restricted Management Access",
- používať silné a komplexné používateľské heslá.
Administrátorom odporúčame bezodkladne aplikovať postup v odporúčaniach výrobcu, sledovať jeho stránky a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-065-0

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

Identifikátor

SIPROTEC 4 and SIPROTEC Compact Multiple Vulnerabilities

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje prúdové ochrany Siprotec a komunikačné moduly EN100, ktoré opravujú viacero bezpečnostných zraniteľností. Najvážnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na modifikáciu firmvéru zasiahnutých zariadení.

Dátum prvého zverejnenia varovania

08.03.2018

CVE

CVE-2018-4838, CVE-2018-4839, CVE-2018-4840

Zasiahnuté systémy

EN100
SIPROTEC 4
SIPROTEC Compact, DIGSI 4

Následky

Neoprávnená zmena v systéme

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame bezodkladne aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov ACL.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-845879.pdf
https://cert-portal.siemens.com/productcert/pdf/ssa-203306.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel Multiple Vulnerabilities

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť v komponente Network File System (NFS) server spočíva v nedostatočnej implementácii mechanizmov riadenia prístupu k NFS serveru a vzdialený útočník by ju mohol zneužiť na získanie prístupu k citlivým údajom a ich modifikáciu.

Dátum prvého zverejnenia varovania

22.01.2018 (posledná aktualizácia 09.03.2018)

CVE

CVE-2018-1000026, CVE-2018-1000028, CVE-2018-7740, CVE-2018-7755, CVE-2018-7757, CVE-2017-18222, CVE-2017-18221, CVE-2018-7995, CVE-2017-18224

Zasiahnuté systémy

Linux Kernel

Následky

Neoprávnená zmena v systéme, Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=1995266727fa8143897e89b55f5d3c79aa828420
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8914a595110a6eca69a5e275b323f5d09e18f4f9
https://tools.cisco.com/security/center/viewAlert.x?alertId=57147
https://tools.cisco.com/security/center/viewAlert.x?alertId=57144
https://tools.cisco.com/security/center/viewAlert.x?alertId=57176
https://tools.cisco.com/security/center/viewAlert.x?alertId=57178

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.0**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Git Client Input Validation Error Vulnerability

Popis

Klient systému Git obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu.
Zraniteľnosť spočíva v nedostatočnom overovaní správ prijatých z Git servera. Správy zo škodlivého Git servera môžu obsahovať ANSI escape kódy, ktoré klient priamo smeruje do terminálu.

Dátum prvého zverejnenia varovania

08.03.2018

CVE

CVE-2018-1000021

Zasiahnuté systémy

Git verzie 2.10.0 až 2.10.5, 2.11.0 až 2.11.4, 2.12.0 až 2.12.4, 2.13.0 až 2.13.6, 2.14.0 až 2.14.3 , 2.15.0 až 2.15.1

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=57136

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.9**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Joyent SmartOS DTrace DOF Out-Of-Bounds Write Privilege Escalation Vulnerability

Popis

Spoločnosť Joyent vydala bezpečnostnú aktualizáciu na svoje virtualizačné prostredie SmartOS, ktorá opravuje bezpečnostnú zraniteľnosť v spracovaní DTrace DOF súborov. Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a lokálny útočník by ju prostredníctvom podvrhnutia upravených DTrace DOF súborov mohol zneužiť na vykonanie škodlivého kódu a následnú eskaláciu privilégií.

Dátum prvého zverejnenia varovania

07.03.2018

CVE

CVE-2018-1171

Zasiahnuté systémy

SmartOS

Následky

Vykonanie škodlivého kódu, Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-18-236/
https://help.joyent.com/hc/en-us/articles/360000608188

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

Identifikátor

Django Multiple Vulnerabilities

Popis

Webový framework Django obsahuje viacero zraniteľností, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služieb. Zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov prostredníctvom regulárnych výrazov.
Prvá skupina zraniteľností sa nachádza vo funkcii *django.utils.html.urlize()*.
Druhá skupina zraniteľností sa nachádza v metódach *chars()* a *words()* v rámci procesu *django.utils.text.Truncator*.

Dátum prvého zverejnenia varovania

06.03.2018 (posledná aktualizácia 12.03.2018)

CVE

CVE-2018-7536 , CVE-2018-7537

Zasiahnuté systémy

Django master branch
Django 2.0.0 až 2.0.2
Django 1.11.8 až 1.11.10
Django verzie 1.8.0 až 1.8.18

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše webové aplikácie nie sú založené na frameworku Django v zraniteľných verziách. V prípade, že áno, zabezpečte aktualizáciu frameworku.

Zdroje

https://www.djangoproject.com/weblog/2018/mar/06/security-releases/
https://tools.cisco.com/security/center/viewAlert.x?alertId=57171
https://tools.cisco.com/security/center/viewAlert.x?alertId=57172