BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 11. 2018 - 04. 12. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome Stable Channel Update	Vysoká	**8.8**
02.	Perl Multiple Vulnerabilities	Vysoká	**8.1**
03.	RubyGems Multiple Vulnerabilities	Vysoká	**7.8**
04.	Wireshark Multiple Denial of Service Vulnerabilities	Vysoká	**7.5**
05.	Netgate pfSense Mutiple Remote Code Injection Vulnerabilities	Vysoká	**7.2**
06.	Linux Kernel Multiple Vulnerabilites	Vysoká	**7.0**
07.	Omron CX-One Code Execution Vulnerabilities	Stredná	**6.6**
08.	INVT Electric VT-Designer Remote Code Execution	Stredná	**6.3**
09.	SpiderControl SCADA WebServer Reflected XSS Vulnerability	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-196

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

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností v internetovom prehliadači Chrome.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu v kontexte webového prehliadača a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.12.2018

CVE

CVE-2018-17480, CVE-2018-17481, CVE-2018-18335, CVE-2018-18336, CVE-2018-18337, CVE-2018-18338, CVE-2018-18339, CVE-2018-18340, CVE-2018-18341, CVE-2018-18342, CVE-2018-18343, CVE-2018-18344, CVE-2018-18345, CVE-2018-18346, CVE-2018-18347, CVE-2018-18348, CVE-2018-18349, CVE-2018-18350, CVE-2018-18351, CVE-2018-18352, CVE-2018-18353, CVE-2018-18354, CVE-2018-18355, CVE-2018-18356, CVE-2018-18357, CVE-2018-18358, CVE-2018-18359

Zasiahnuté systémy

Google Chrome verzie staršie ako 71.0.3578.80

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://chromereleases.googleblog.com/search/label/Stable%20updates

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

Identifikátor

Perl Multiple Vulnerabilities

Popis

Perl.org vydala bezpečnostné aktualizácie na Perl, ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nesprávnej implementácii pamäťových operácií v rámci funkcie S_regatom v regcomp.c a útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených regulárnych výrazov mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ďalšiu zraniteľnosť vo funkncii Perl_my_setenv() by lokálny autentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.
Posledná zraniteľnosť spočíva v nesprávnom vyhodnocovaní regulárnych výrazov v rámci funkcie S_grok_bslash_N v regcomp.c a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného regulárneho výrazu mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.
Na uvedené zraniteľnosti je voľne dostupný PoC (Proof of Concept) kód.

Dátum prvého zverejnenia varovania

03.12.2018

CVE

CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314

Zasiahnuté systémy

Perl verzie pred 5.28.1

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59232
https://tools.cisco.com/security/center/viewAlert.x?alertId=59233
https://tools.cisco.com/security/center/viewAlert.x?alertId=59234
https://tools.cisco.com/security/center/viewAlert.x?alertId=59235

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

Identifikátor

RubyGems Multiple Vulnerabilities

Popis

RubyGems.org vydala bezpečnostnú aktualizáciu na produkt RubyGems, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nesprávnej implementácii deserializácie objektov a lokálny útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného YAML súboru mohol zneužiť na vykonanie škodlivého kódu.
Druhá zraniteľnosť spočíva v nedostatočnom overovaní kryptografických podpisov v package.rb a vzdialený neautentifikovaný útočník by ju mohol zneužiť na inštaláciu škodlivých RubyGems gemov.
Ostatné zraniteľnosti by lokálny neautentifikovaný útočník mohol zneužiť na vykonanie neoprávnených zmien v systéme alebo na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.11.2018

CVE

CVE-2018-1000073, CVE-2018-1000074, CVE-2018-1000075, CVE-2018-1000076

Zasiahnuté systémy

RubyGems verzie staršie ako 2.7.6

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59212
https://tools.cisco.com/security/center/viewAlert.x?alertId=59213
https://tools.cisco.com/security/center/viewAlert.x?alertId=59214
https://tools.cisco.com/security/center/viewAlert.x?alertId=59215

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

Identifikátor

Wireshark Multiple Denial of Service Vulnerabilities

Popis

Vývojári analytického nástroja Wireshark vydali aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo sieťovej prevádzky mohol zneužiť na zneprístupnenie služieb na zasiahnutom systéme.
Zraniteľnosti sa nachádzajú v komponentoch:
- IxVeriWave file parser
- ZigBee Cluster Library (ZCL) dissector
- Wireshark dissection engine
- Multimedia Messaging Service Encapsulation (MMSE) dissector
- Parallel Virtual File System (PVFS) dissector
- Distributed Component Object Model (DCOM) dissector
- LBMPDM dissector

Dátum prvého zverejnenia varovania

27.11.2018

CVE

CVE-2018-19622, CVE-2018-19623, CVE-2018-19624, CVE-2018-19625, CVE-2018-19626, CVE-2018-19627, CVE-2018-19628

Zasiahnuté systémy

Wireshark verzie 2.6.0 až 2.6.4, 2.4.0 až 2.4.10

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.wireshark.org/security/wnpa-sec-2018-51.html
https://www.wireshark.org/security/wnpa-sec-2018-52.html
https://www.wireshark.org/security/wnpa-sec-2018-53.html
https://www.wireshark.org/security/wnpa-sec-2018-54.html
https://www.wireshark.org/security/wnpa-sec-2018-55.html
https://www.wireshark.org/security/wnpa-sec-2018-56.html
https://www.wireshark.org/security/wnpa-sec-2018-57.html

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

Identifikátor

Netgate pfSense Mutiple Remote Code Injection Vulnerabilities

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostných zraniteľnostiach v produkte pfSense. Zraniteľnosti nachádzajúce sa v skripte system_advanced_misc.php spočívajú v nedostatočnom overovaní POST parametrov (powerd_normal_mode, powerd_ac_mode, powerd_battery_mode) a vzdialený autentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených POST požiadaviek mohol zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

03.12.2018

CVE

CVE-2018-4019, CVE-2018-4020, CVE-2018-4021

Zasiahnuté systémy

Netgate pfSense verzie CE 2.4.4-RELEASE

Následky

Vykonanie škodlivého kódu a úplné 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 zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0690

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

Identifikátor

Linux Kernel Multiple Vulnerabilites

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nedostatočnom overovaní chybových stavov vo funkcii usb_audio_probe definovanej v sound/usb/card.c a lokálny autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Druhá zraniteľnosť spočíva v nedostatočnom overovaní vstupov vo funkcii ip_frag_reasm() v net/ipv4/ip_fragment.c a neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente by ju prostredníctvom podvrhnutia defragmentovaných paketov mohol zneužiť na zneprístupnenie služby.
Ostatné zraniteľnosti by lokálny autentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.11.2018

CVE

CVE-2018-14641, CVE-2018-14646, CVE-2018-17977, CVE-2018-19824

Zasiahnuté systémy

Linux Kernel

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59210
https://tools.cisco.com/security/center/viewAlert.x?alertId=59199
https://tools.cisco.com/security/center/viewAlert.x?alertId=59197
https://tools.cisco.com/security/center/viewAlert.x?alertId=59242

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Omron CX-One Code Execution Vulnerabilities

Popis

Spoločnosť Omron vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch série CX-One.
Bezpečnostné zraniteľnosti spočívajú v nesprávnej implementácii mechanizmov práce s pamäťou a lokálny neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

04.12.2018

CVE

CVE-2018-18989, CVE-2018-18993

Zasiahnuté systémy

Omron CX-One verzie 4.42 a staršie
Omron CX-Programmer verzie 9.66 a staršie
Omron CX-Server verzie 5.0.23 a staršie

Následky

Zneprístupnenie služby, Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-338-01

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

Identifikátor

INVT Electric VT-Designer Remote Code Execution

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostných zraniteľnostiach v produkte INVT Electric VT-Designer.
Bezpečnostné zraniteľnosti spočívajúce v nedostatočnom overovaní používateľských vstupov by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby alebo vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

29.11.2018

CVE

CVE-2018-18983, CVE-2018-18987

Zasiahnuté systémy

VT-Designer verzie 2.1.7.31

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame riadiace systémy a jednotky prevádzkovať úplne oddelené od Internetu, sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-333-01

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

Identifikátor

SpiderControl SCADA WebServer Reflected XSS Vulnerability

Popis

Spoločnosť SpiderControl vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte SCADA WebServer.
Bližšie nešpecifikovanú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených URL obsahujúcich JavaScript zneužiť na realizáciu XSS (Cross-Site Scripting) útoku.

Dátum prvého zverejnenia varovania

04.12.2018

CVE

CVE-2018-18991

Zasiahnuté systémy

SpiderControl SCADA WebServer verzie staršie ako 2.03.0001

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-338-02