BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 08. 2018 – 04. 09. 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-125

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

Identifikátor

Multiple Code Execution Vulnerabilities in Micro Focus Products

Popis

Spoločnosť Micro Focus vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostné zraniteľnosti v produktoch Data Center Automation Containerized (DCA) Suite, Operations Bridge Containerized Suite, Service Management Automation, Network Operations Management (NOM) Suite a Hybrid Cloud Management Containerized Suite.
Bližšie nešpecifikované zraniteľnosti by neautentifikovaný útočník nachádzajúci sa v rovnakom sieťovom segmente mohol prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek zneužiť na vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

30.08.2018

CVE

CVE-2018-6498, CVE-2018-6499

Zasiahnuté systémy

Micro Focus Data Center Automation Containerized Suite verzie 2017.01 až 2018.05
Micro Focus Operations Bridge Containerized Suite verzie 2017.11, 2018.02, 2018.05
Micro Focus Service Management Automation verzie 2017.11, 2018.02, 2018.05
Network Operations Management Suite verzie 2017.11, 2018.02, and 2018.05
Micro Focus Hybrid Cloud Management Containerized Suite verzie 2017.08, 2017.11, 2018.02, 2018.05

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03236632
https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03236648
https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03236667
https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03236669
https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03236678
https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03236722

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

Identifikátor

Multiple Vulnerabilities in Trend Micro Security and OfficeScan

Popis

Spoločnosť Trend Micro vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v produktoch Trend Micro Security a OfficeScan.
Zraniteľnosti v produktoch Trend Micro Security spočívajú v nesprávnom spracovávaní ID_AMSP_MASTER požiadaviek v rámci procesu coreServiceShell.exe a lokálny neautentifikovaný útočník by ich mohol zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad zasiahnutým systémom.
Zraniteľnosť v produkte OfficeScan nachádzajúca sa v Ntrtscan.exe spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený útočník by ju mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

23.08.2018 (posledná aktualizácia 30.08.2018)

CVE

CVE-2018-10513, CVE-2018-10514, CVE-2018-15363, CVE-2018-15364

Zasiahnuté systémy

Trend Micro Premium Security verzie staršie ako 12.0.1226
Trend Micro Maximum Security verzie staršie ako 12.0.1226
Trend Micro Internet Security verzie staršie ako 12.0.1226
Trend Micro Antivirus + Security verzie staršie ako 12.0.1226
Trend Micro OfficeScan verzie XG (12.0)

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://esupport.trendmicro.com/en-US/home/pages/technical-support/1120742.aspx
https://success.trendmicro.com/solution/1120678

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

Identifikátor

Cisco Data Center Network Manager Path Traversal Vulnerability

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte Cisco Data Center Network Manager.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v rámci manažmentového rozhrania a vzdialený autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek obsahujúcich /../ sekvencie mohol zneužiť na vykonanie neoprávnených zmien v systéme a získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

28.08.2018

CVE

CVE-2018-0464

Zasiahnuté systémy

Cisco Data Center Network Manager verzie staršie ako 11.0(1)

Následky

Neoprávnená zmena v systéme, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180828-dcnm-traversal

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

Identifikátor

Dropbox Code Execution Vulnerability

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte Dropbox, ktorá spočíva v nesprávnej implementácii nahrávania DLL knižníc.
Zraniteľnosť by lokálny autentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

24.08.2018 (posledná aktualizácia 28.08.2018)

CVE

-

Zasiahnuté systémy

Dropbox verzie 54.5.90

Následky

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

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/148982

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

Identifikátor

Linux Kernel Local Privilege Escalation Vulnerability

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť nachádzajúcu sa v podsystéme crypto.
Bezpečnostná zraniteľnosť spočíva v implementačnej chybe a lokálny autentifikovaný útočník by ju mohol zneužiť na eskaláciu privilégií a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.08.2018

CVE

CVE-2018-14619

Zasiahnuté systémy

Linux kernel verzie 4.15-rc3 a staršie

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58847
https://exchange.xforce.ibmcloud.com/vulnerabilities/148951
http://seclists.org/oss-sec/2018/q3/184

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

Identifikátor

RSA BSAFE Micro Edition Suite Multiple Vulnerabilities

Popis

Spoločnosť RSA vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch RSA BSAFE Micro Edition Suite a RSA BSAFE Crypto-C Micro Edition.
Najzávažnejšie zraniteľnosti spočívajú v implementačnej chybe ASN.1 parsera a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvorených ASN.1 dát mohol zneužiť na zneprístupnenie služby.
Zraniteľnosť CVE-2018-11057 v BSAFE Micro Edition Suite by vzdialený neautentifikovaný útočník mohol prostredníctvom Bleichenbacher-ovho útoku zneužiť na získanie RSA kľúča a neoprávnený prístup k citlivým údajom.
Zraniteľnosť CVE-2018-11055 v BSAFE Micro Edition Suite by lokálny autentifikovaný útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

28.08.2018

CVE

CVE-2018-11054, CVE-2018-11055, CVE-2018-11056, CVE-2018-11057, CVE-2018-11058

Zasiahnuté systémy

RSA BSAFE Crypto-C Micro Edition verzie staršie ako 4.0.5.3
RSA BSAFE Micro Edition Suite verzie staršie ako 4.0.11
RSA BSAFE Micro Edition Suite verzie staršie ako 4.1.6.1

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://seclists.org/fulldisclosure/2018/Aug/46
https://exchange.xforce.ibmcloud.com/vulnerabilities/149081
https://exchange.xforce.ibmcloud.com/vulnerabilities/149082
https://exchange.xforce.ibmcloud.com/vulnerabilities/149083
https://exchange.xforce.ibmcloud.com/vulnerabilities/149084
https://exchange.xforce.ibmcloud.com/vulnerabilities/149085

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

Identifikátor

Episerver 7 Information Disclosure Vulnerability

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte Episerver 7 patch 4, ktorá spočíva v nedostatočnom overovaní používateľských vstupov.
Zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvoreného XML súboru mohol zneužiť na realizáciu XXE (XML External Entity) útoku a následné získanie prístupu k citlivým údajom.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

29.08.2018

CVE

CVE-2017-17762

Zasiahnuté systémy

Episerver Episerver 7 patch 4

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na systéme pre správu obsahu Episerver 7. V prípade, že áno, odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/149120
https://www.exploit-db.com/exploits/45286/

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

Identifikátor

HPE Intelligent Management Center Remote Arbitrary File Modification

Popis

Spoločnosť Hewlett Packard vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero zraniteľností v produkte HPE Intelligent Management Center.
Bezpečnostná zraniteľnosť v komponente imciccdm spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na vytvorenie súborov na zasiahnutom systéme.
Druhá zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v komponente TFTP server a vzdialený neautentifikovaný útočník by ju mohol zneužiť na odstránenie súborov prístupných používateľovi Administrator.

Dátum prvého zverejnenia varovania

27.08.2018

CVE

CVE-2018-7102

Zasiahnuté systémy

HPE Intelligent Management Center (iMC) Plat 7.3 E0506P09

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03887en_us
https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-hpesbhf03872en_us
https://www.zerodayinitiative.com/advisories/ZDI-18-966/
https://www.zerodayinitiative.com/advisories/ZDI-18-955/

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:
- Bluetooth Attribute Protocol (ATT) dissector (epan/dissectors/packet-btatt.c)
- Radiotap dissector (epan/dissectors/packet-ieee80211-radiotap-iter.c)
- Audio/Video Distribution Transport Protocol (AVDTP) dissector (epan/dissectors/packet-btavdtp.c)
Na uvedené zraniteľnosti je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

29.08.2018 (posledná aktualizácia 30.08.2018)

CVE

CVE-2018-16056, CVE-2018-16057, CVE-2018-16058

Zasiahnuté systémy

Wireshark verzie 2.2.0 až 2.2.16, 2.4.0 až 2.4.8, 2.6.0 až 2.6.2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu systémov.

Zdroje

https://www.wireshark.org/security/wnpa-sec-2018-44.html
https://www.wireshark.org/security/wnpa-sec-2018-45.html
https://www.wireshark.org/security/wnpa-sec-2018-46.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=58841
https://tools.cisco.com/security/center/viewAlert.x?alertId=58842
https://tools.cisco.com/security/center/viewAlert.x?alertId=58843

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

Identifikátor

Joomla! Multiple Vulnerabilities

Popis

Vývojári systému pre správu obsahu Joomla! vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností nachádzajúcich sa v jadre systému.
Najzávažnejšia zraniteľnosť spočíva v nesprávnej implementácii triedy InputFilter využívanej pri uploade súborov a vzdialený autentifikovaný útočník by ju mohol prostredníctvom podvrhnutia špeciálne vytvorených PHAR súborov zneužiť na vykonanie škodlivého kódu.
Ďalšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.

Dátum prvého zverejnenia varovania

29.08.2018

CVE

CVE-2018-15880, CVE-2018-15881, CVE-2018-15882

Zasiahnuté systémy

Joomla! verzie 1.5.0 až 3.8.11

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na systéme pre správu obsahu Joomla! v zraniteľných verziách. V prípade, že áno, preverte integritu systému a prístupové logy na prítomnosť neoprávnených zmien a následne zabezpečte aktualizáciu systému na najnovšiu verziu.

Zdroje

https://developer.joomla.org/security-centre/744-20180802-core-stored-xss-vulnerability-in-the-frontend-profile.html
https://developer.joomla.org/security-centre/743-20180801-core-hardening-the-inputfilter-for-phar-stubs.html
https://developer.joomla.org/security-centre/745-20180803-core-acl-violation-in-custom-fields.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-joomla-could-allow-for-arbitrary-code-execution_2018-094/

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

Identifikátor

PostgreSQL JDBC Driver Man-in-the-Middle Attack Vulnerability

Popis

Vývojári databázového systému PostgreSQL vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v implementácii JDBC Java Database Connectivity (JDBC) ovládača.
Zraniteľnosť spočíva v nedostatočnom overovaní parametra hostname a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených SSL certifikátov mohol zneužiť na realizáciu MITM (Man-in-The-Middle) útoku a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

27.08.2018 (posledná aktualizácia 31.08.2018)

CVE

CVE-2018-10936

Zasiahnuté systémy

PostgreSQL JDBC Driver verzie staršie ako 42.2.5

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.postgresql.org/about/news/1883/
https://exchange.xforce.ibmcloud.com/vulnerabilities/149157

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

QEMU Denial of Service Vulnerability

Popis

Vývojári virtualizačnej platformy QEMU vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť spočívajúcu v implementačnej chybe v rámci komponentu seccomp sandbox.
Zraniteľnosť nachádzajúcu sa v qemu-seccomp.c by lokálny autentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek mohol zneužiť na vyvolanie pádu VM(Virtual Machine) a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.08.2018

CVE

CVE-2018-15746

Zasiahnuté systémy

QEMU

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/148956

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

Identifikátor

WhatsApp Denial of Service Vulnerability

Popis

Bezpečnostní výskumníci informovali o bezpečnostnej zraniteľnosti v produkte WhatsApp pre zariadenia s operačným systémom iOS.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorenej sekvencie UTF-8 znakov mohol zneužiť na poškodenie pamäte a následné zneprístupnenie služby.
Na uvedenú zraniteľnosť je voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

24.08.2018 (posledná aktualizácia 28.08.2018)

CVE

-

Zasiahnuté systémy

WhatsApp verzie 2.18.61 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Používateľom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

http://www.openwall.com/lists/oss-security/2018/08/28/6
https://exchange.xforce.ibmcloud.com/vulnerabilities/148953
https://packetstormsecurity.com/files/149122