BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 06. 2018 – 03. 07. 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-083

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

Identifikátor

Micro Focus Secure Messaging Gateway Multiple Vulnerabilities

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností v produkte Secure Messaging Gateway (SMG).

Zraniteľnosť v komponentoch *web administration* a *quarantine* by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie SQL injekcie a následne zobraziť, pridať, upraviť alebo odstrániť údaje uložené v backend databáze. Uvedená zraniteľnosť útočníkovi umožňuje vytvoriť používateľský účet s administrátorskými právami.

Druhá zraniteľnosť sa nachádza v komponente *web administration* a vzdialený autentifikovaný útočník by ju mohol zneužiť na vykonanie škodlivého kódu na SMG serveri.

Dátum prvého zverejnenia varovania

27.06.2018 (posledná aktualizácia 29.06.2018)

CVE

CVE-2018-12464, CVE-2018-12465

Zasiahnuté systémy

Micro Focus Secure Messaging Gateway verzie staršie ako 471

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Následne odporúčame preveriť integritu databázy a prístupové logy na prítomnosť pokusov o SQL injekciu.

Zdroje

https://support.microfocus.com/kb/doc.php?id=7023132
https://support.microfocus.com/kb/doc.php?id=7023133
https://exchange.xforce.ibmcloud.com/vulnerabilities/145598
https://exchange.xforce.ibmcloud.com/vulnerabilities/145599

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

Identifikátor

Mozilla Firefox and Firefox ESR Multiple Vulnerabilities

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú 18 zraniteľností v produktoch Firefox a Firefox ESR.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.06.2018

CVE

CVE-2018-12358, CVE-2018-12359, CVE-2018-12360, CVE-2018-12361, CVE-2018-12362, CVE-2018-12363, CVE-2018-12364, CVE-2018-12365, CVE-2018-12366, CVE-2018-12367, CVE-2018-12368, CVE-2018-12369, CVE-2018-12370, CVE-2018-12371, CVE-2018-5156, CVE-2018-5186, CVE-2018-5187, CVE-2018-5188,

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 61, ESR 60.1 a ESR 52.9

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2018-17/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-firefox-could-allow-for-arbitrary-code-execution_2018-072/

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

Identifikátor

Multiple Vulnerabilities in PHP Could Allow for Arbitrary Code Execution

Popis

Vývojári skriptovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá rieši viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.06.2018

CVE

CVE-2018-12882 a ďalšie

Zasiahnuté systémy

PHP 7.2 verzie staršie ako 7.2.7
PHP 7.1 verzie staršie ako 7.1.19

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-php-could-allow-for-arbitrary-code-execution_2018-071/
https://tools.cisco.com/security/center/viewAlert.x?alertId=58300

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.2**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware ESXi, Workstation, and Fusion Multiple Out-of-bounds Read Vulnerabilities

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na svoje produkty ESXi, Workstation, a Fusion, ktoré opravujú viacero bezpečnostných zraniteľností v komponente *shader translator*.
Bezpečnostné zraniteľnosti umožňujú vzdialenému autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služieb na zasiahnutom systéme a tiež získať prístup k citlivým informáciám.

Dátum prvého zverejnenia varovania

28.06.2018

CVE

CVE-2018-6965, CVE-2018-6966, CVE-2018-6967

Zasiahnuté systémy

VMware ESXi 6.7
VMware Workstation 14.x
VMware Fusion 10.x pre OS X

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0016.html
https://www.securityweek.com/vulnerabilities-patched-vmware-esxi-workstation-fusion
https://www.vulnerabilitycenter.com/#!vul=87166

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

Identifikátor

Polaris Office Remote Code Execution Vulnerability

Popis

Spoločnosť Polaris vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v kancelárskom balíku Polaris Office.
Zraniteľnosť spočíva v nesprávnej implementácii načítavania dynamických knižníc .DLL a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvoreného .DLL súboru mohol zneužiť na vykonanie škodlivého kódu.
Pre uvedenú zraniteľnosť je voľne dostupný exploit.

Dátum prvého zverejnenia varovania

26.06.2018

CVE

CVE-2018-12589

Zasiahnuté systémy

Polaris Office 2017 v8

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/145494
https://packetstormsecurity.com/files/148312

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

Identifikátor

Zoho ManageEngine Desktop Central Arbitraty File Deletion Vulnerability

Popis

Produkt Zoho ManageEngine Desktop Central obsahuje bezpečnostnú zraniteľnosť, ktorá spočíva v nedostatočnej implementácii mechanizmov riadenia prístupu v servlete *AgentTrayIconServlet*.
Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálnych požiadaviek zneužiť na odstránenie súborov na webovom serveri.

Dátum prvého zverejnenia varovania

20.06.2018 (posledná aktualizácia 29.06.2018)

CVE

CVE-2018-12999

Zasiahnuté systémy

Zoho ManageEngine Desktop Central verzie 10.0.255

Následky

Neoprávnená zmena v systéme

Odporúčania

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

Zdroje

https://github.com/unh3x/just4cve/issues/9
https://exchange.xforce.ibmcloud.com/vulnerabilities/145597

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

Identifikátor

HPE Integrated Lights-Out Code Execution Vulnerability

Popis

Spoločnosť Hewlett Packard vydala aktualizáciu, ktorá rieši bezpečnostnú zraniteľnosť v produkte Integrated Lights Out.
Bližšie nešpecifikovanú zraniteľnosť by vzdialený autentifikovaný útočník s administrátorskými právami mohol zneužiť na úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.06.2018 (posledná aktualizácia 30.06.2018)

CVE

CVE-2018-7078

Zasiahnuté systémy

HPE Integrated Lights-Out 5 (iLO 5) pre servery HPE Gen10 verzie staršie ako 1.30
HPE Integrated Lights-Out 4 (iLO 4) verzie staršie ako 2.60

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým systémom a ich funkciám zavedením zoznamu pre riadenie prístupov (ACL)

Zdroje

https://support.hpe.com/hpsc/doc/public/display?docId=hpesbhf03844en_us
https://exchange.xforce.ibmcloud.com/vulnerabilities/145457

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Medtronic MyCareLink Patient Monitor Multiple Vulnerabilities

Popis

Spoločnosť Medtronic vydala bezpečnostnú aktualizáciu, ktorá opravuje dve bezpečnostné zraniteľnosti v produkte MyCareLink Patient Monitor slúžiacom na monitoring srdcových implantátov.
Prvá zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a neautentifikovaný útočník s fyzickým prístupom k zariadeniu by ju mohol zneužiť na získanie prístupu do operačného systému zariadenia.
Druhá zraniteľnosť spočíva v skutočnosti, že zariadenie obsahuje debugovací kód slúžiaci na testovanie komunikácie medzi monitorom a implantátmi. Útočník s fyzickým prístupom k monitorovaciemu zariadeniu a pacientovi s implantátom by debugovací kód mohol zneužiť na prístup a modifikáciu údajov v pamäti srdcového implantátu.

Dátum prvého zverejnenia varovania

28.06.2018

CVE

CVE-2018-8868, CVE-2018-8870

Zasiahnuté systémy

Medtronic MyCareLink Patient Monitor model 24950, 24952

Následky

Neoprávnený prístup do systému, Neoprávnená zmena v systéme

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Po ich vydaní sa záplaty inštalujú v rámci automatickej aktualizácie softvéru zariadenia. Výrobca taktiež odporúča limitovať fyzický prístup k zariadeniam.

Zdroje

http://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic-MyCareLink-Security-Bulletin_FNL.pdf
https://ics-cert.us-cert.gov/advisories/ICSMA-18-179-01

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

Identifikátor

Eclipse Jetty Multiple Vulnerabilities

Popis

Vývojári webového servera Eclipse Jetty vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v súčasti *FileSessionDataStore* a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia session ID získať existujúce HTTP sessions a tiež spôsobiť zneprístupnenie služieb na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

29.06.2018

CVE

CVE-2018-12536, CVE-2017-7658, CVE-2018-12538, CVE-2017-7657, CVE-2017-7656

Zasiahnuté systémy

Eclipse Jetty verzie staršie ako 9.4.9.v20180320, 9.2.25.v2018060 a 9.3.24.v20180605

Následky

Neoprávnený prístup k citlivým údajom, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58311
https://tools.cisco.com/security/center/viewAlert.x?alertId=58312
https://tools.cisco.com/security/center/viewAlert.x?alertId=58313
https://tools.cisco.com/security/center/viewAlert.x?alertId=58314
https://tools.cisco.com/security/center/viewAlert.x?alertId=58315

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

Identifikátor

Avalanche 6.2.2 Security Patch

Popis

Spoločnosť Ivanti vydala bezpečnostnú aktualizáciu na svoj produkt Avalanche, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu autentifikovanému útočníkovi získať prístup k autentifikačným údajom používateľov systému.

Dátum prvého zverejnenia varovania

19.06.2018

CVE

CVE-2018-8901, CVE-2018-8902

Zasiahnuté systémy

Avalanche verzie staršie ako 6.2.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://community.ivanti.com/docs/DOC-68406
https://community.ivanti.com/servlet/JiveServlet/download/68406-2-62121/CVE-2018-8902_PublicStatement.pdf
https://community.ivanti.com/servlet/JiveServlet/download/68406-2-62122/CVE-2018-8901_Public%20Statement.pdf

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

Identifikátor

MISP UsersController.php Security Bypass

Popis

Vývojári platformy MISP vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii *app/Controller/UsersController.php*.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravenej HTTP požiadavky obísť zabezpečenie systému voči brute-force útoku.

Dátum prvého zverejnenia varovania

21.06.2018

CVE

CVE-2018-12649

Zasiahnuté systémy

MISP 2.4.92

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://cert.civis.net/en/index.php?action=alert&param=CVE-2018-12649
https://exchange.xforce.ibmcloud.com/vulnerabilities/145247