BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 08. 2018 – 28. 08. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Adobe Photoshop and Creative Cloud Desktop Application Multiple Vulnerabilities	Vysoká	**8.8**
02.	Microsoft Windows Task Scheduler Local Privilege Escalation Vulnerability	Vysoká	**8.8**
03.	Multiple Vulnerabilities in Siemens SIMATIC STEP 7, SIMATIC WinCC and Automation License Manager	Vysoká	**8.8**
04.	Ansible Tower Cross-Site Request Forgery Vulnerability	Vysoká	**8.8**
05.	Couchbase Server REST API Code Execution Vulnerability	Vysoká	**8.8**
06.	Yokogawa iDefine, STARDOM, ASTPLANNER and TriFellows Buffer Overflow Vulnerability	Vysoká	**8.6**
07.	Apache ActiveMQ, Sentry, Cayenne Vulnerabilities	Vysoká	**8.3**
08.	Ghostscript Contains Multiple -dSAFER Sandbox Bypass Vulnerabilities	Vysoká	**7.3**
09.	Schneider Electric Modicon M221 Multiple Vulnerabilities	Vysoká	**7.1**
10.	phpMyAdmin XSS Vulnerability	Stredná	**6.1**
11.	IBM WebSphere Application Server Liberty Information Disclosure Vulnerability	Stredná	**5.9**

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-122

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

Identifikátor

Adobe Photoshop and Creative Cloud Desktop Application Multiple Vulnerabilities

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie, ktoré opravujú viaceré zraniteľnosti v produktoch Adobe Photoshop a Adobe Creative Cloud Desktop Application.
Bližšie nešpecifikované zraniteľnosti v Adobe Photoshop by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne vytvorených súborov zneužiť poškodenie pamäte a následné vykonanie škodlivého kódu v kontexte prihláseného používateľa.
Bezpečnostná zraniteľnosť v Adobe Creative Cloud Desktop Application spočíva v nesprávnom overovaní certifikátov a útočník by ju mohol zneužiť na eskaláciu privilégií na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

21.08.2018 (posledná aktualizácia 28.08.2018)

CVE

CVE-2018-12810, CVE-2018-12811, CVE-2018-12829

Zasiahnuté systémy

Photoshop CC 2017 verzie 18.1.5 a staršie
Photoshop CC 2018 verzie 19.1.5 a staršie
Creative Cloud Desktop Application verzie 4.6.0 a staršie

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/photoshop/apsb18-28.html
https://helpx.adobe.com/security/products/creative-cloud/apsb18-32.html

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

Identifikátor

Microsoft Windows Task Scheduler Local Privilege Escalation Vulnerability

Popis

Bezpečnostní výskumníci a CERT/CC informovali o zero-day bezpečnostnej zraniteľnosti nachádzajúcej sa v plánovači úloh (Task Scheduler) na systémoch Microsoft Windows.
Bezpečnostná zraniteľnosť v rozhraní Advanced Local Procedure Call (ALPC) spočíva nesprávnej implementácii mechanizmov riadenia prístupu a lokálny autentifikovaný útočník by ju prostredníctvom špeciálne vytvoreného .job súboru mohol zneužiť na eskaláciu privilégií a získanie úplnej kontroly nad zasiahnutým systémom.
Na uvedenú zraniteľnosť je voľne dostupný exploit, ktorého funkčnosť bola overená na 64-bitových verziách Windows 10 a Windows Server 2016.

Dátum prvého zverejnenia varovania

27.08.2018 (posledná aktualizácia 28.08.2018)

CVE

-

Zasiahnuté systémy

Microsoft Windows

Následky

Eskalácia privilégií

Odporúčania

Spoločnosť Microsoft v súčasnej dobe pracuje na vydaní aktualizácií. Odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://www.kb.cert.org/vuls/id/906424
https://exchange.xforce.ibmcloud.com/vulnerabilities/148942
https://www.theregister.co.uk/2018/08/28/windows_zero_day_lpe/

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

Identifikátor

Multiple Vulnerabilities in Siemens SIMATIC STEP 7, SIMATIC WinCC and Automation License Manager

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie, ktoré riešia bezpečnostné zraniteľnosti v produktoch Automation License Manager (ALM), SIMATIC STEP 7 a SIMATIC WinCC.
Bližšie nešpecifikovanú zraniteľnosť v ALM by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Druhú zraniteľnosť v ALM by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených paketov mohol zneužiť na skenovanie otvorených portov na systémoch prístupných zo zasiahnutého zariadenia.
Zraniteľnosti v produktoch SIMATIC STEP 7 a SIMATIC WinCC sa nachádzajú v softvéri TIA Portal (Totally Integrated Automation) a spočívajú v nesprávnej konfigurácii oprávnení v počiatočnej inštalácii TIA Portal. Lokálny neautentifikovaný útočník by uvedené zraniteľnosti mohol zneužiť na vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.08.2018

CVE

CVE-2018-11453
CVE-2018-11454
CVE-2018-11455
CVE-2018-11456

Zasiahnuté systémy

Automation License Manager 5: verzie staršie ako 5.3.4.4
Automation License Manager 6: verzie staršie ako 6.0.1 (len CVE-2018-11455)
SIMATIC STEP 7 (TIA Portal), WinCC (TIA Portal) V10, V11, V12: všetky verzie
SIMATIC STEP 7 (TIA Portal), WinCC (TIA Portal) V13: všetky verzie
SIMATIC STEP 7 (TIA Portal), WinCC (TIA Portal) V14: verzie staršie ako V14 SP1 Update 6
SIMATIC STEP 7 (TIA Portal), WinCC (TIA Portal) V15: verzie staršie ako V15 Update 2

Následky

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

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Administrátorom produktov SIMATIC STEP 7 a SIMATIC WinCC spoločnosť Siemens odporúča: - limitovať prístup k operačnému systému zariadení len na autorizovaný personál - spracovávať len GSD súbory pochádzajúce z dôveryhodných zdrojov

Zdroje
https://cert-portal.siemens.com/productcert/pdf/ssa-920962.pdf https://cert-portal.siemens.com/productcert/pdf/ssa-979106.pdf

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

Identifikátor

Ansible Tower Cross-Site Request Forgery Vulnerability

Popis

Produkt Red Hat Ansible Tower obsahuje bezpečnostnú zraniteľnosť, ktorá je spôsobená nedostatočným overovaním používateľských vstupov v skripte awx/authentication.py. Uvedenú zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia škodlivého webového obsahu mohol zneužiť na vykonanie CSRF (Cross-Site Request Forgery) a XSS (Cross-Site Scripting) útokov a následné vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

22.08.2018

CVE

CVE-2018-10884

Zasiahnuté systémy

Ansible Tower 3.1.8
Ansible Tower 3.2.6

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Odporúčame limitovať prístup k zasiahnutým systémom len na dôveryhodných administrátorov, sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/148723
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10884

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

Identifikátor

Couchbase Server REST API Code Execution Vulnerability

Popis

Produkt Couchbase Server obsahuje bezpečnostnú zraniteľnosť, ktorá je spôsobená nesprávnym riadením prístupu k REST API produktu.
Vzdialený autentifikovaný útočník by zraniteľnosť prostredníctvom podvrhnutia kódu programovacieho jazyka Erlang mohol zneužiť na vykonanie škodlivého kódu s oprávneniami používateľa, ktorý spustil Couchbase.

Dátum prvého zverejnenia varovania

23.08.2018

CVE

CVE-2018-15728

Zasiahnuté systémy

Couchbase Server

Následky

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

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/148760
http://seclists.org/bugtraq/2018/Aug/49
https://packetstormsecurity.com/files/149068

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Yokogawa iDefine, STARDOM, ASTPLANNER and TriFellows Buffer Overflow Vulnerability

Popis

Spoločnosť Yokogawa vydala bezpečnostné aktualizácie, ktoré opravujú bezpečnostnú zraniteľnosť v produktoch iDefine, STARDOM, ASTPLANNER and TriFellows.
Bližšie nešpecifikovaná zraniteľnosť sa nachádza vo funkcii licence management a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených dát mohol zneužiť na vyvolanie pretečenia zásobníka a následné vykonanie škodlivého kódu alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.08.2018

CVE

CVE-2018-0651

Zasiahnuté systémy

ASTPLANNER verzie R15.01 a staršie
iDefine for ProSafe-RS verzie R1.16.3 a staršie
STARDOM VDS verzie R7.50 a staršie
STARDOM FCN/FCJ Simulator verzie R4.20 a staršie
TriFellows verzie 5.04 a staršie

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov. Tiež odporúčame prevádzkovať riadiace jednotky a systémy úplne oddelené od Internetu. Ak to nie je možné, odporúčame zavedením firewallových pravidiel limitovať dostupnosť riadiacich jednotiek a systémov z Internetu.

Zdroje

https://web-material3.yokogawa.com/YSAR-18-0006-E.pdf
https://ics-cert.us-cert.gov/advisories/ICSA-18-233-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache ActiveMQ, Sentry, Cayenne Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie, ktoré opravujú viaceré bezpečnostné zraniteľnosti v produktoch ActiveMQ, Sentry a Cayenne.
Najzávažnejšia je bezpečnostná zraniteľnosť v Apache Sentry, ktorá spočíva v nedostatočnej implementácie bezpečnostných mechanizmov a vzdialený autentifikovaný útočník by ju mohol zneužiť na neoprávnený prístup a modifikáciu údajov v tabuľkách chránených prostredníctvom Sentry.
Zraniteľnosť v Apache ActiveMQ spočíva v nedostatočnom overovaní používateľských vstupov v queues.jsp a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených URL mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku, vykonanie škodlivého kódu vo webovom prehliadači a získanie prístupu k údajom uloženým v cookies, vrátane autentifikačných údajov.
Zraniteľnosť v Apache Cayenne spočíva v implementačnej chybe XML parsera v nástroji CayenneModeler GUI a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených XML súborov mohol zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

22.08.2018

CVE

CVE-2018-8006, CVE-2018-8028, CVE-2018-11758

Zasiahnuté systémy

Apache Sentry verzie 2.0.0
Apache ActiveMQ verzie staršie ako 5.15.5
Apache Cayenne verzie 3.1, 3.1.1, 3.1.2, 3.2.M1, 4.0.M2 to 4.0.M5, 4.0.B1, 4.0.B2, 4.0.RC1, 4.1.M1

Následky

Vykonanie škodlivého kódu, Neoprávnená zmena v systéme, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://exchange.xforce.ibmcloud.com/vulnerabilities/148809 https://exchange.xforce.ibmcloud.com/vulnerabilities/148808 https://exchange.xforce.ibmcloud.com/vulnerabilities/148759 http://seclists.org/oss-sec/2018/q3/169 http://seclists.org/oss-sec/2018/q3/151 https://www.trustwave.com/Resources/Security-Advisories/Advisories/TWSL2018-008/?fid=11632

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Ghostscript Contains Multiple -dSAFER Sandbox Bypass Vulnerabilities

Popis

Bezpečnostní výskumníci vydali upozornenie na bezpečnostnú zraniteľnosť v Ghostscript, ktorá umožňuje obísť sandboxové bezpečnostné mechanizmy.
Ghostscript obsahuje voliteľnú funkcionalitu -dSAFER, ktorej hlavnou úlohou je zabrániť vykonaniu nebezpečných PostScript operácií. Na základe výskumu ale viacero PostScript operácií obchádza bezpečnostné mechanizmy -dSAFER, čo vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného obsahu umožňuje vykonať škodlivý kód.
Zraniteľnosť je možné zneužiť vo všetkých systémoch a aplikáciách, ktoré využívajú Ghostscript, ako napr. populárne ImageMagick, GraphicsMagick, GIMP, Evince, alebo Okular.
Na uvedenú zraniteľnosť je voľne dostupný exploit.

Dátum prvého zverejnenia varovania

21.08.2018 (posledná aktualizácia 25.08.2018)

CVE

-

Zasiahnuté systémy

Všetky systémy a aplikácie využívajúce Ghostscript

Následky

Vykonanie škodlivého kódu

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú Ghostscript. V prípade, že áno, odporúčame Vám:
- **ak je to možné, odstrániť Ghostscript**
Nakoľko sú voľne dostupné exploity pre rozličné útočné vektory, najefektívnejším postupom je dočasné odstránenie Ghostscript zo systémov.
- **ImageMagick útočný vektor eliminovať vypnutím PS, EPS, PDF a XPS kóderov**
ImageMagick štandardne využíva Ghostscript na spracovanie PostScript-ového obsahu. Prostredníctvom bezpečnostných politík definovaných v policy.xml možno vypnúť spracovanie PS, EPS, PDF a XPS obsahu.
- ak prevádzkujete mail2fax bránu, odporúčame ju do doby vydania aktualizácie odpojiť od Internetu

- ak zdieľate tlačiarne z počítača s operačným systémom Linux alebo Mac OS po sieti, odporúčame toto zdieľanie vypnúť
- sledovať stránky výrobcov a po vydaní bezpečnostných záplat vykonať aktualizáciu

Zdroje
https://www.kb.cert.org/vuls/id/332928
http://seclists.org/oss-sec/2018/q3/142
http://openwall.com/lists/oss-security/2018/08/21/2

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Schneider Electric Modicon M221 Multiple Vulnerabilities

Popis

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie, ktoré opravujú viaceré bezpečnostné zraniteľnosti v PLC jednotkách Modicon M221.
Najzávažnejšie sú bližšie nešpecifikované zraniteľnosti spočívajúce v nesprávnej implementácii bezpečnostných a autentifikačných mechanizmov. Vzdialený neautentifikovaný útočník by ich mohol zneužiť na získanie neoprávneného prístup do systému, upload a vykonanie škodlivého kódu z PLC.
Ďalšiu zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených rámcov mohol zneužiť na vyvolanie reštartu zariadenia a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.08.2018 (posledná aktualizácia 23.08.2018)

CVE

CVE-2018-7789, CVE-2018-7790, CVE-2018-7791, CVE-2018-7792

Zasiahnuté systémy

Modicon M221 verzie firmvéru staršie ako V1.6.2.0

Následky

Neoprávnený prístup do systému, Neoprávnená zmena v systéme, Vykonanie škodlivého kódu, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame prevádzkovať riadiace jednotky a systémy úplne oddelené od Internetu. Ak to nie je možné, odporúčame zavedením firewallových pravidiel limitovať dostupnosť riadiacich jednotiek a systémov z Internetu.

Zdroje

https://www.schneider-electric.com/en/download/document/SEVD-2018-233-01/
https://www.schneider-electric.com/en/download/document/SEVD-2018-235-01/

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

Identifikátor

phpMyAdmin XSS Vulnerability

Popis

Vývojári phpMyAdmin vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente file import.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný 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

23.08.2018

CVE

CVE-2018-15605

Zasiahnuté systémy

phpMyAdmin verzie 4.x staršie ako

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame limitovať prístup k rozhraniu phpMyAdmin zavedením zoznamu pre riadenie prístupov (ACL), napríklad uloženým v .htaccess súbore.

Zdroje

https://www.phpmyadmin.net/security/PMASA-2018-5/
https://www.securitytracker.com/id/1041548
https://tools.cisco.com/security/center/viewAlert.x?alertId=58786

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

Identifikátor

IBM WebSphere Application Server Liberty Information Disclosure Vulnerability

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu, ktorá opravuje zraniteľnosť v produkte IBM WebSphere Application Server Liberty.
Zraniteľnosť spočíva v nesprávnom prenose pri využití Java Authentication SPI for Containers (JASPIC) a vzdialený neautentifikovaný útočník by ju mohol zneužiť na neoprávnený prístup k citlivým údajom.
Zraniteľnosť je možné zneužiť len keď nastavenia aplikačného servera umožňujú prístup prostredníctvom nezabezpečeného HTTP a autentifikačných mechanizmov JASPIC alebo JSR375.

Dátum prvého zverejnenia varovania

22.08.2018

CVE

CVE-2018-1755

Zasiahnuté systémy

IBM WebSphere Application Server Liberty

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=ibm10728689
https://exchange.xforce.ibmcloud.com/vulnerabilities/148597
https://securitytracker.com/id/1041558