BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 05. 2018 – 05. 06. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apple Releases Security Updates	Vysoká	**8.8**
02.	Chrome Stable Channel Update for Desktop	Vysoká	**8.8**
03.	Git Submodule Name Validation Flaw	Vysoká	**8.8**
04.	Multiple Huawei Server Products Vulnerabilities	Vysoká	**8.8**
05.	VMWare Horizon Client for Linux Privilege Escalation	Vysoká	**8.4**
06.	RSA Web Threat Detection SQL Injection Vulnerability	Vysoká	**7.6**
07.	F5 BIG-IP Multiple Vulnerabilities	Vysoká	**7.5**
08.	QNAP Proxy Server Multiple Vulnerabilities	Vysoká	**7.5**
09.	Natus Xltek EEG NeuroWorks Multiple Denial of Service Vulnerabilities	Vysoká	**7.5**
10.	Delta Industrial Automation DOPSoft Multiple Vulnerabilities	Vysoká	**7.3**
11.	GE MDS PulseNET Multiple Vulnerabilities	Vysoká	**7.3**
12.	Synology Drive Multiple Vulnerabilities	Stredná	**6.5**
13.	IBM Security Guardium Big Data Intelligence (SonarG) Multiple 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-067

BEZPEČNOSTNÝ BULLETIN

Týždeň 30. 05. 2018 – 05. 06. 2018

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

Identifikátor

Apple Releases Security Updates

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty macOS, iOS, watchOS, tvOS, iCloud pre Windows, iTunes pre Windows a Safari, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti v operačných systémoch macOS High Sierra a OS X El Capitan sa nachádzajú v jadre a v súčastiach FontParser, Hypervisor, IOFireWireAVC, IOGraphics, IOHIDFamily, NVIDIA Graphics Driver, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.
Zraniteľnosti v ostatných produktoch by vzdialený neautentifikovaný útočník zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby alebo neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

01.06.2018

CVE

CVE-2018-4141, CVE-2018-4159, CVE-2018-4171, CVE-2018-4184, CVE-2018-4188, CVE-2018-4190, CVE-2018-4192, CVE-2018-4193, CVE-2018-4196, CVE-2018-4198, CVE-2018-4199, CVE-2018-4200, CVE-2018-4201, CVE-2018-4202, CVE-2018-4204, CVE-2018-4205, CVE-2018-4206, CVE-2018-4211, CVE-2018-4214, CVE-2018-4215, CVE-2018-4218, CVE-2018-4219, CVE-2018-4221, CVE-2018-4222, CVE-2018-4223, CVE-2018-4224, CVE-2018-4225, CVE-2018-4226, CVE-2018-4227, CVE-2018-4228, CVE-2018-4229, CVE-2018-4230, CVE-2018-4232, CVE-2018-4233, CVE-2018-4234, CVE-2018-4235, CVE-2018-4236, CVE-2018-4237, CVE-2018-4238, CVE-2018-4239, CVE-2018-4240, CVE-2018-4241, CVE-2018-4242, CVE-2018-4243, CVE-2018-4244, CVE-2018-4246, CVE-2018-4247, CVE-2018-4249, CVE-2018-4250, CVE-2018-4251, CVE-2018-4252, CVE-2018-4253

Zasiahnuté systémy

macOS High Sierra 10.12.6, 10.13.4
OS X El Capitan 10.11.6
iOS verzie staršie ako 11.4
Safari verzie staršie ako 11.1.1
iCloud for Windows verzie staršie ako 7.5
watchOS verzie staršie ako 4.3.1
iTunes for Windows verzie staršie ako 12.7.5
tvOS verzie staršie ako 11.4

Následky

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

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-067

Odporúčania
Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://support.apple.com/en-us/HT208848
https://support.apple.com/en-us/HT208849
https://support.apple.com/en-us/HT208850
https://support.apple.com/en-us/HT208851
https://support.apple.com/en-us/HT208852
https://support.apple.com/en-us/HT208853
https://support.apple.com/en-us/HT208854
https://isc.sans.edu/diary/rss/23727

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

Identifikátor

Chrome Stable Channel Update for Desktop

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu, ktorá rieši viacero chýb a 34 bezpečnostných zraniteľností v internetovom prehliadači Chrome.
Najvážnejšie bezpečnostné zraniteľnosti v komponentoch Blink a Skia by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia škodlivého webového obsahu zneužiť na vykonanie škodlivého kódu v kontexte webového prehliadača a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.05.2018

CVE

CVE-2018-6123, CVE-2018-6124, CVE-2018-6125, CVE-2018-6126, CVE-2018-6127, CVE-2018-6128, CVE-2018-6129, CVE-2018-6130, CVE-2018-6131, CVE-2018-6132, CVE-2018-6133, CVE-2018-6134, CVE-2018-6135, CVE-2018-6136, CVE-2018-6137, CVE-2018-6138, CVE-2018-6139, CVE-2018-6140, CVE-2018-6141, CVE-2018-6142, CVE-2018-6143, CVE-2018-6144, CVE-2018-6145, CVE-2018-6147

Zasiahnuté systémy

Google Chrome verzie staršie ako 67.0.3396.62

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://chromereleases.googleblog.com/search/label/Stable%20updates
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2018-059/
https://www.securitytracker.com/id/1041014

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

Identifikátor

Git Submodule Name Validation Flaw

Popis

Vývojári systému správy Git vydali aktualizáciu svojho produktu, ktorá rieši viaceré bezpečnostné zraniteľnosti.
Najvážnejšia bezpečnostná zraniteľnosť sa nachádza v module names a spočíva v nedostatočnom overovaní používateľských vstupov zasiahnutým systémom a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených repozitárov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

29.05.2018

CVE

CVE-2018-11233, CVE-2018-11235

Zasiahnuté systémy

Git 2.13
Git 2.14.x staršie ako 2.14.4
Git 2.15.x staršie ako 2.15.2
Git 2.16.x staršie ako 2.16.4
Git 2.17.x staršie ako 2.17.1

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.securitytracker.com/id/1040991
https://access.redhat.com/security/cve/cve-2018-11235

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

Identifikátor

Multiple Huawei Server Products Vulnerabilities

Popis

Spoločnosť Huawei vydala bezpečnostné aktualizácie, ktoré opravujú viacero zraniteľností v Huawei serveroch.
Najzávažnejšia je dvojica bezpečnostných zraniteľností, ktoré spočívajú v nedostatočnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ich mohol prostredníctvom podvrhnutia špeciálne vytvorených JSON požiadaviek zneužiť na modifikáciu prístupového hesla administrátorského účtu a eskaláciu privilégií v napadnutom systéme. Ďalšia zraniteľnosť v komponente iBMC (intelligent Baseboard Managament Controller) spočíva v nesprávnej implementácii mechanizmov autentifikácie a vzdialený neautentifikovaný útočník by ju mohol prostredníctvom podvrhnutia špeciálne vytvorených prihlasovacích správ zneužiť na neoprávnený prístup k citlivým údajom a modifikáciu prihlasovacích údajov ostatných používateľov systému.

Dátum prvého zverejnenia varovania

30.05.2018

CVE

CVE-2018-7943, CVE-2018-7949, CVE-2018-7950, CVE-2018-7951

Zasiahnuté systémy

Huawei 1288H V5 verzie V100R005C00, 2288H V5 verzie V100R005C00, 2488 V5 verzie V100R005C00, CH121 V3/V5 verzie V100R001C00, CH121L V3/V5 verzie V100R001C00, CH140 V3 verzie V100R001C00, CH140L V3 verzie V100R001C00, CH220 V3 verzie V100R001C00, CH222 V3 verzie V100R001C00, CH242 V3/V5 verzie V100R001C00, RH1288 V3 verzie V100R003C00, RH2288 V3 verzie V100R003C00, RH2288H V3 verzie V100R003C00, XH310 V3 verzie V100R003C00, XH321 V3 verzie V100R003C00, XH321 V5 verzie V100R005C00, XH620 V3 verzie V100R003C00

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180530-01-server-en
http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180530-02-server-en
http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180530-03-server-en

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

Identifikátor

VMWare Horizon Client for Linux Privilege Escalation

Popis

Spoločnosť VMWare vydala bezpečnostnú aktualizáciu, ktoré rieši bezpečnostnú zraniteľnosť v produkte VMWare Horizon Client.
Zraniteľnosť spočívajúcu v nesprávnom využívaní funkcie Set User ID by lokálny neautentifikovaný útočník mohol zneužiť na eskaláciu privilégií na úroveň root.

Dátum prvého zverejnenia varovania

29.05.2018

CVE

CVE-2018-6964

Zasiahnuté systémy

VMware Horizon Client verzie 4.x a staršie bežiace na platforme Linux

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0014.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/144088

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

RSA Web Threat Detection SQL Injection Vulnerability

Popis

Spoločnosť RSA vydala bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť v produkte RSA Web Threat Detection.
Zraniteľnosť spočívajúcu v nedostatočnom overovaní používateľských vstupov v moduloch Administration a Forensics by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie SQL injekcie a získať neoprávnený prístup k citlivým údajom v backend databáze.

Dátum prvého zverejnenia varovania

31.05.2018

CVE

CVE-2018-1252

Zasiahnuté systémy

RSA Web Threat Detection verzie staršie ako 6.4

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

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

Zdroje

http://seclists.org/fulldisclosure/2018/Jun/4
https://securitytracker.com/id/1041026

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

Identifikátor

F5 BIG-IP Multiple Vulnerabilities

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na svoje produkty BIG-IP, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia zraniteľnosť spočíva v nesprávnom spracovaní paketov počas TLS handshake-u v komponente TMM (Traffic Management Microkernel) a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálnej sekvencie paketov mohol zneužiť na zneprístupnenie služby. Uvedenú zraniteľnosť je možné zneužiť len na zariadeniach so zapnutou funkciou Proxy SSL.

Zraniteľnosť v BIG-IP ASM by vzdialený neautentifikovaný útočník mohol zneužiť na vyradenie behaviorálnej DoS ochrany a následne spôsobiť zneprístupnenie služieb.

Ďalšia zraniteľnosť nachádzajúca sa v komponente GeoIP Lookup spočíva v nedostatočnom filtrovaní HTML kódu v používateľských vstupoch a vzdialený autentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a získať prístup k údajom obete uloženým v cookies vrátane autentifikačných údajov.

Zraniteľnosť vo virtuálnych serveroch využívajúcich modul HSM (Hardware Security Module) by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne upravených TLS požiadaviek zneužiť na zneprístupnenie služby.

BIG-IP systémy v režime Forward Proxy využívajúce funkciu inflate obsahujú bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne upravených dát zneužiť na realizáciu Zip Bomb útoku a následné zneprístupnenie služby.

Poslednú zraniteľnosť v nástroji BIG-IP Configuration by vzdialený autentifikovaný útočník mohol zneužiť na zobrazenie súborov obsahujúcich továrenské údaje.

Dátum prvého zverejnenia varovania

31.05.2018

CVE

CVE-2017-6153, CVE-2018-5513, CVE-2018-5521, CVE-2018-5522, CVE-2018-5523, CVE-2018-5524, CVE-2018-5525, CVE-2018-5526

Zasiahnuté systémy

BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, GTM, Link Controller, PEM, WebAccelerator, WebSafe) verzie 11.2.1 - 11.5.5, 11.6.1 - 11.6.3, 12.1.0 - 12.1.3, 13.0.0, 13.1.0

BIG-IP (ASM) verzie 13.1.0

Enterprise Manager verzie 3.1.1

Následky
Zneprístupnenie služby, Neoprávnená zmena v systéme

Odporúčania
Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://support.f5.com/csp/article/K46940010
https://support.f5.com/csp/article/K23124150
https://support.f5.com/csp/article/K50254952
https://support.f5.com/csp/article/K53931245
https://support.f5.com/csp/article/K00363258
https://support.f5.com/csp/article/K62201098
https://support.f5.com/csp/article/K52167636
https://support.f5.com/csp/article/K54130510

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

Identifikátor

QNAP Proxy Server Multiple Vulnerabilities

Popis

Spoločnosť QNAP vydala aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produkte QNAP Proxy Server.

Najzávažnejšia zraniteľnosť je spôsobená nesprávnym filtrovaním HTML kódu v používateľských vstupoch a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených súborov mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a získať prístup k autentifikačným údajom obete uloženým v cookies.

Ďalšiu zraniteľnosť by vzdialený neautentifikovaný útočník prostredníctvom CSRF (Cross-Site Request Forgery) útoku mohol zneužiť na vykonanie príkazov v kontexte prihláseného používateľa.

Ostatné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a vzdialený neautentifikovaný útočník by ich mohol zneužiť na úpravu nastavení aplikácie Proxy Server.

Dátum prvého zverejnenia varovania

01.06.2018

CVE

CVE-2017-7635, CVE-2017-7636, CVE-2017-7637, CVE-2017-7639

Zasiahnuté systémy

QNAP Proxy Server verzie 1.2.0 a staršie

Následky

Vykonanie škodlivého kódu, Neoprávnená modifikácia systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.qnap.com/en/security-advisory/nas-201806-01
https://www.securitytracker.com/id/1041025

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

Identifikátor

Natus Xltek EEG NeuroWorks Multiple Denial of Service Vulnerabilities

Popis

Výskumníci Cisco TALOS zverejnili informácie o bezpečnostných zraniteľnostiach v NeuroWorks 8, sieťovom komponente systému pre elektroencefalografiu Xltek EEG od spoločnosti Natus.
Zraniteľnosti spočívajú v nesprávnej implementácie deserializácie a prechádzania zabudovaných údajových štruktúr (itemlist, KeyTree) a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne upravených paketov mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

31.05.2018

CVE

CVE-2017-2852, CVE-2017-2858, CVE-2017-2860

Zasiahnuté systémy

Natus Xltek NeuroWorks 8

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0354
https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0362
https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0364

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

Identifikátor

Delta Industrial Automation DOPSoft Multiple Vulnerabilities

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu, ktorá upravuje viacero bezpečnostných zraniteľností v produkte DOPSoft.
Uvedené zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne upravených .dpa súborov zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby alebo neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

31.05.2018

CVE

CVE-2018-10617, CVE-2018-10621, CVE-2018-10623

Zasiahnuté systémy

DOPSoft verzie 4.00.04 a staršie

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-151-01

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

Identifikátor

GE MDS PulseNET Multiple Vulnerabilities

Popis

Spoločnosť GE vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produktoch GE PulseNET a GE PulseNET Enterprise.
Najzávažnejšia zraniteľnosť spočíva v nesprávnej implementácii mechanizmov autentifikácie a je spôsobená chybou v JAVA RMI (Remote Method Invocation) vstupnom porte. Vzdialený neautentifikovaný útočník by ju mohol zneužiť na získanie prístupu do systému, spustenie aplikácií a vykonanie škodlivého kódu prostredníctvom webových služieb systému.
Ďalšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu viacerých variant XXE (XML External Entity) útoku a získať neoprávnený prístup k citlivým údajom.
Poslednú bezpečnostnú zraniteľnosť by vzdialený autentifikovaný útočník mohol zneužiť na neoprávnený prístup alebo zmazanie súborov uložených v systéme.

Dátum prvého zverejnenia varovania

31.05.2018

CVE

CVE-2018-10611, CVE-2018-10613, CVE-2018-10615

Zasiahnuté systémy

GE PulseNET verzie 3.2.1 a staršie
GE PulseNET Enterprise verzie 3.2.1 a staršie

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-151-02
https://www.cybersecurity-help.cz/vdb/SB2018060107

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Synology Drive Multiple Vulnerabilities

Popis

Spoločnosť Synology vydala bezpečnostnú aktualizáciu na svoj produkt Synology Drive, ktorá rieši viaceré bezpečnostné zraniteľnosti.
Najvážnejšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v komponente File Sharing Notify Toast a vzdialený autentifikovaný útočník by ju mohol prostredníctvom podvrhnutia špeciálne pripraveného názvu súboru zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

01.06.2018

CVE

CVE-2018-8921, CVE-2018-8922

Zasiahnuté systémy

Synology Drive verzie staršie ako 1.0.2-10275

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.synology.com/en-global/support/security/Synology_SA_18_11

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

Identifikátor

IBM Security Guardium Big Data Intelligence (SonarG) Multiple Vulnerability

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Security Guardium Big Data Intelligence (SonarG), ktorá opravuje viacero bezpečnostných zraniteľností v administrátorskej konzole.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných opatrení a umožňuje vzdialenému neautentifikovanému útočníkovi získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

24.05.2018

CVE

CVE-2018-1375, CVE-2018-1376, CVE-2018-1370

Zasiahnuté systémy

IBM Security Guardium Big Data Intelligence (SonarG) verzie staršie ako 3.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www-01.ibm.com/support/docview.wss?uid=swg22016512
http://www-01.ibm.com/support/docview.wss?uid=swg22016132
http://www-01.ibm.com/support/docview.wss?uid=swg22016513