BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 05. 2018 – 08. 05. 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-049

BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 05. 2018 – 08. 05. 2018

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

Identifikátor

Android Security Bulletin—May 2018

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj operačný systém Android, ktoré opravujú 23 rôznych bezpečnostných zraniteľností.
Najvážnejšími sú zraniteľnosti v komponentoch Nvidia a Qualcomm, ktoré umožňujú lokálnemu útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť vykonanie škodlivého kódu v kontexte privilegovaného procesu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.05.2018

CVE

CVE-2017-13077, CVE-2017-13309, CVE-2017-13310, CVE-2017-13311, CVE-2017-13312, CVE-2017-13313, CVE-2017-13314, CVE-2017-13315, CVE-2017-16643, CVE-2017-18154, CVE-2017-5715, CVE-2017-5754, CVE-2017-6289, CVE-2017-6293, CVE-2018-3562, CVE-2018-3565, CVE-2018-3578, CVE-2018-3580, CVE-2018-5840, CVE-2018-5841, CVE-2018-5845, CVE-2018-5846, CVE-2018-5850

Zasiahnuté systémy

Operačný systém Android

Následky

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

Odporúčania

Používateľom a administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://source.android.com/security/bulletin/2018-05-01
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-arbitrary-code-execution_2018-051/

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

Identifikátor

Microsoft Windows Host Compute Service Shim Code Execution

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj operačný systém Windows, ktorá opravuje bezpečnostnú zraniteľnosť v knižnici Windows Host Compute Service Shim (hcsshim).
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

02.05.2018

CVE

CVE-2018-8115

Zasiahnuté systémy

Microsoft Windows Host Compute Service Shim 0.6.9 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8115
https://exchange.xforce.ibmcloud.com/vulnerabilities/142697

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

Identifikátor

Swift for Ubuntu Privilege Escalation

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na programovací nástroj Swift pre Ubuntu, ktorá opravuje zraniteľnosť spočívajúcu v nesprávnom nahrávaní knižníc.
Bezpečnostná zraniteľnosť umožňuje lokálnemu útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

04.05.2018

CVE

CVE-2018-4220

Zasiahnuté systémy

Swift verzie nižšie ako 4.1.1 pre Ubuntu 14.04

Následky

Eskalácia privilégií, Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT208804
https://lists.apple.com/archives/security-announce/2018/May/msg00000.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/142821

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

Identifikátor

Philips Brilliance Computed Tomography (CT) System Vulnerabilities

Popis

Spoločnosť Philips vydala upozornenie na bezpečnostné zraniteľnosti, ktoré sa nachádzajú v CT systémoch Brilliance.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu neautentifikovanému útočníkovi eskalovať svoje privilégiá na napadnutom systéme.

Dátum prvého zverejnenia varovania

03.05.2018

CVE

CVE-2018-8853, CVE-2018-8861, CVE-2018-8857

Zasiahnuté systémy

Brilliance 64 verzia 2.6.2 a staršie
Brilliance iCT verzia 4.1.6 a staršie
Brillance iCT SP verzia 3.2.4 a staršie
Brilliance CT Big Bore verzia 2.3.5 a staršie

Následky

Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam. Spoločnosť Philips tiež odporúča za účelom získania dodatočných informácií kontaktovať lokálneho Philips distribútora.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-123-01

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

Identifikátor

A Vulnerability in 7-Zip Could Allow for Arbitrary Code Execution

Popis

Vývojári slobodného komprimačného softvéru 7-Zip vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť v komponente *CPP/7zip/Archive/Rar/RarHandler.cpp*.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou inicializáciou štruktúr a umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia upravených komprimovaných súborov vyvolať chyby v pamäti a následne vykonať škodlivý kód v kontexte prihláseného používateľa.

Dátum prvého zverejnenia varovania

01.05.2018

CVE

CVE-2018-10115

Zasiahnuté systémy

7-Zip verzie staršie ako 18.05

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov. Nová verzia 7zip nielenže opravuje túto zraniteľnosť, ale navyše pridáva ochranu technikou ASLR, ktorá urobí zneužitie podobných zraniteľností ťažším.

Zdroje

https://landave.io/2018/05/7-zip-from-uninitialized-memory-to-remote-code-execution/
https://www.cisecurity.org/advisory/a-vulnerability-in-7-zip-could-allow-for-arbitrary-code-execution_2018-049/

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

Identifikátor

.NET Security Vulnerability in Siveillance VMS

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj video softvér Siveillance VMS, ktorá opravuje bezpečnostnú zraniteľnosť v Recording Server, Management Server, a Management Client.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou mechanizmov zabezpečenia a umožňuje vzdialenému útočníkovi eskalovať svoje privilégiá a spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

03.05.2018

CVE

CVE-2018-7891

Zasiahnuté systémy

Siveillance VMS 2016 R1 verzie nižšie ako V10.0a
Siveillance VMS 2016 R2 verzie nižšie ako V10.1a
Siveillance VMS 2016 R3 verzie nižšie ako V10.2b
Siveillance VMS 2017 R1 verzie nižšie ako V11.1a
Siveillance VMS 2017 R2 verzie nižšie ako V11.2a
Siveillance VMS 2018 R1 verzie nižšie ako V12.1a
XProtect Corporate; XProtect Essential+; XProtect Expert; XProtect Express+; XProtect Professional+

Následky

Eskalácia privilégií, Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov. Zneužitiu uvedenej zraniteľnosti sa dá predísť zablokovaním sieťového prístupu k portom 7474/TCP a 9993/TCP na zasiahnutých produktoch.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-457058.pdf
https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Symantec Norton Core Command Execution

Popis

Spoločnosť Symantec vydala bezpečnostnú aktualizáciu na svoje routre Norton Core, ktorá opravuje bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje útočníkovi v lokálnej sieti vykonať škodlivé príkazy na napadnutom zariadení.

Dátum prvého zverejnenia varovania

30.04.2018

CVE

CVE-2018-5234

Zasiahnuté systémy

Symantec Norton Core staršie ako v237

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne aktualizovať zasiahnuté systémy.

Zdroje

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20180430_00
https://exchange.xforce.ibmcloud.com/vulnerabilities/142611

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

Identifikátor

Dell EMC ECOM XML External Entity Injection Vulnerability

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoje produkty Dell EMC, ktorá opravuje bezpečnostnú zraniteľnosť v komponente EMC Common Object Manager (ECOM). Bezpečnostná zraniteľnosť je spôsobená nesprávnou konfiguráciou XML parsera a umožňuje vzdialenému autentifikovanému útočníkovi prostredníctvom špeciálne vytvorených XML súborov získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.04.2018

CVE

CVE-2018-1183

Zasiahnuté systémy

Dell EMC Unisphere for VMAX Virtual Appliance verzie staršie ako 8.4.0.8
Dell EMC Solutions Enabler Virtual Appliance verzie staršie ako 8.4.0.8
Dell EMC VASA Provider Virtual Appliance verzie staršie ako 8.4.0.512
Dell EMC SMIS verzie staršie ako 8.4.0.6
Dell EMC VMAX Embedded Management (eManagement) 1.4.0.347 a staršie
Dell EMC VNX1 Operating Environment; Dell EMC VNX2 Operating Environment
Dell EMC VNXe3200 Operating Environment (OE)
Dell EMC VNXe1600 Operating Environment (OE) verzie staršie ako 3.1.9.9570228
Dell EMC VNXe 3100/3150/3300 Operating Environment (OE)
Dell EMC ViPR SRM verzie 3.7, 3.7.1, 3.7.2, 4.0, 4.0.1, 4.0.2, 4.0.3
Dell EMC XtremIO verzie 4.x; Dell EMC VMAX eNAS verzie 8.x
Dell EMC Unity Operating Environment (OE) verzie staršie ako 4.3.0.1522077968

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://seclists.org/fulldisclosure/2018/Apr/61

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

Identifikátor

Apache Derby Externally Controlled Input Vulnerability

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache Derby, ktorá opravuje bezpečnostnú zraniteľnosť v komponente Network Server.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou mechanizmov zabezpečenia a umožňuje vzdialenému útočníkovi prostredníctvom špeciálne vytvorených paketov získať neoprávnený prístup do zasiahnutého systému.

Dátum prvého zverejnenia varovania

05.05.2018

CVE

CVE-2018-1313

Zasiahnuté systémy

Apache Derby verzie staršie ako 10.14.2.0

Následky

Neoprávnený prístup do systému

Odporúčania

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

Zdroje

https://db.apache.org/derby/releases/release-10.14.2.0.cgi
http://www.systemtek.co.uk/2018/05/apache-derby-externally-controlled-input-vulnerability-cve-2018-1313/
https://access.redhat.com/security/cve/cve-2018-1313

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

Identifikátor

F5 BIG-IP HTTP/2 Request Processing Flaw Lets Remote Users Cause the Target TMM Component to Crash

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť je spôsobená nesprávnym overovaním používateľských vstupov v Traffic Management Microkernel a umožňuje vzdialenému útočníkovi pomocou podvrhnutia špeciálne upravených HTTP/2 požiadaviek spôsobiť reštart systému a zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

01.05.2018

CVE

CVE-2018-5514, CVE-2018-5515, CVE-2018-5516, CVE-2018-5519

Zasiahnuté systémy

BIG-IP verzie nižšie ako 13.1.0.6

Následky

Zneprístupnenie služby, Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://support.f5.com/csp/article/K45320419
https://securitytracker.com/id?1040804
https://exchange.xforce.ibmcloud.com/vulnerabilities/142677
https://support.f5.com/csp/article/K46121888
https://tools.cisco.com/security/center/viewAlert.x?alertId=57702

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

Identifikátor

RSA Authentication Manager Vulnerabilities

Popis

Spoločnosť RSA vydala bezpečnostnú aktualizáciu na svoj produkt RSA Authentication Manager, ktorá opravuje viacero bezpečnostných zraniteľností v Security Console.
Bezpečnostné zraniteľnosti sú spôsobené nesprávnym spracovaním používateľských vstupov a umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť zneprístupnenie služieb a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

04.05.2018

CVE

CVE-2018-1247, CVE-2018-1248

Zasiahnuté systémy

RSA Authentication Manager verzie staršie ako 8.3 P1
RSA Authentication Manager web-tier server verzie staršie ako 8.3 P1

Následky

Zneprístupnenie služby, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://seclists.org/fulldisclosure/2018/May/18
https://exchange.xforce.ibmcloud.com/vulnerabilities/142857
https://exchange.xforce.ibmcloud.com/vulnerabilities/142856