BEZPEČNOSTNÝ BULLETIN

Týždeň 31. 10. 2018 - 06. 11. 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-177

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

Identifikátor

Viacero zraniteľností v Apple produktoch

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty Safari 12, iCloud, iTunes, watchOS, iOS, tvOS, macOS Mojave, macOS Sierra, macOS High Sierra, ktoré opravujú viacero bezpečnostných zraniteľností. Najvážnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi vykonať škodlivý kód v kontexte privilegovaného procesu.

Dátum prvého zverejnenia varovania

31.10.2018

CVE

CVE-2017-0898, CVE-2017-10784, CVE-2017-12613, CVE-2017-12618, CVE-2017-14033, CVE-2017-14064, CVE-2017-17405, CVE-2017-17742, CVE-2018-3639, CVE-2018-3640, CVE-2018-3646, CVE-2018-4126, CVE-2018-4153, CVE-2018-4203, CVE-2018-4242, CVE-2018-4259, CVE-2018-4286, CVE-2018-4287, CVE-2018-4288, CVE-2018-4291, CVE-2018-4295, CVE-2018-4304, CVE-2018-4308, CVE-2018-4310, CVE-2018-4326, CVE-2018-4331, CVE-2018-4334, CVE-2018-4340, CVE-2018-4341, CVE-2018-4342, CVE-2018-4346, CVE-2018-4348, CVE-2018-4350, CVE-2018-4354, CVE-2018-4365, CVE-2018-4366, CVE-2018-4367, CVE-2018-4368, CVE-2018-4369, CVE-2018-4371, CVE-2018-4372, CVE-2018-4373, CVE-2018-4374, CVE-2018-4375, CVE-2018-4376, CVE-2018-4377, CVE-2018-4378, CVE-2018-4382, CVE-2018-4384, CVE-2018-4385, CVE-2018-4386, CVE-2018-4387, CVE-2018-4388, CVE-2018-4389, CVE-2018-4390, CVE-2018-4391, CVE-2018-4392, CVE-2018-4393, CVE-2018-4394, CVE-2018-4395, CVE-2018-4396, CVE-2018-4398, CVE-2018-4399, CVE-2018-4400, CVE-2018-4401, CVE-2018-4402, CVE-2018-4403, CVE-2018-4406, CVE-2018-4407, CVE-2018-4408, CVE-2018-4409, CVE-2018-4410, CVE-2018-4411, CVE-2018-4412, CVE-2018-4413, CVE-2018-4415, CVE-2018-4416, CVE-2018-4417, CVE-2018-4418, CVE-2018-4419, CVE-2018-4420, CVE-2018-4422, CVE-2018-4423, CVE-2018-4424, CVE-2018-4425, CVE-2018-4426, CVE-2018-4427, CVE-2018-6797, CVE-2018-6914, CVE-2018-8777, CVE-2018-8778, CVE-2018-8779, CVE-2018-8780

Zasiahnuté systémy

Safari verzie staršie ako 12.0.1
iCloud pre Windows staršie ako verzia 7.8
iTunes verzie staršie ako 12.9.1
watchOS verzie staršie ako 5.1
iOS verzie staršie ako 12.1
tvOS verzie staršie ako 12.1
macOS Mojave verzie staršie ako 10.14.1
macOS Sierra verzie staršie ako 10.12.6, Security Update 2018-005
macOS High Sierra verzie staršie ako 10.13.6, Security Update 2018-001

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov

Zdroje
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2018-120/ https://support.apple.com/en-us/HT209192 https://support.apple.com/en-us/HT209193 https://support.apple.com/en-us/HT209194 https://support.apple.com/en-us/HT209195 https://support.apple.com/en-us/HT209196 https://support.apple.com/en-us/HT209197 https://support.apple.com/en-us/HT209198

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

Identifikátor

GitLab zraniteľnosti

Popis

Spoločnosť GitLab vydala bezpečnostnú aktualizáciu na svoj produkt Gitlab, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajúce v nedostatočnej implementácii bezpečnostných mechanizmov a nedostatočnom overovaní používateľských vstupov by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu (XSS, CSRF, SQL injekcia) a získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

31.10.2018

CVE

CVE-2018-18640, CVE-2018-18641, CVE-2018-18643, CVE-2018-18645, CVE-2018-18646, CVE-2018-18648, CVE-2018-18649

Zasiahnuté systémy

Gitlab verzie staršie ako 11.4.3

Následky

Vykonanie škodlivého kódu, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://www.linuxsecurity.com/content/view/214677?rdf

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

Identifikátor

Dell EMC Integrated Data Protection Appliance zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt Integrated Data Protection Appliance, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v existencii zabudovaných používateľských účtov (support, admin) s predvolenými heslami a vzdialený neautentifikovaný útočník by ju mohol zneužiť na neoprávnený prístup do systému a získanie prístupových práv na čítanie a zápis k určitým systémovým súborom.

Dátum prvého zverejnenia varovania

29.10.2018

CVE

CVE-2018-11062

Zasiahnuté systémy

Dell EMC Integrated Data Protection Appliance verzie 2.0, 2.1, 2.2

Následky

Neoprávnený prístup do systému, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/fulldisclosure/2018/Oct/53

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

Identifikátor

Schneider Electric Software Update (SESU) zraniteľnosť

Popis

Vývojári zo spoločnosti Schneider Electric vydali bezpečnostnú aktualizáciu svojho produktu Schneider Electric Software Update (SESU), ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu autentifikovanému útočníkovi prostredníctvom špeciálne vytvoreného DLL súboru vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

25.10.2018

CVE

CVE-2018-7799

Zasiahnuté systémy

Schneider Electric Software Update (SESU), všetky verzie staršie ako 2.2.0
Nasledovný softvér obsahuje SESU:
Acti 9 Smart Test
AltivarATV320DtmLibrary, AltivarDTMLibrary, AltivarMachine340DTMLibrary
AltivarProcessATV6xxDTMLibrary,AltivarProcessATV9xxDTMLibrary
Blue
CompactNSX Firmware Update
Ecodial Advance Calculation
eConfigure
Ecoreach Software
EcoStruxure Modicon Builder
eXLhoist
Configuration Software
Lexium 26 DTM Library, Lexium 28 DTM Library, Lexium 32 DTM Library, LV Motor Starter
PowerSCADA Expert
Schneider Electric Floating License Manager, Schneider Electric License Manager, Schneider Electric Motion Sizer, Schneider Electric SQL Gateway
SoMachine Basic, SoMachine Motion Software, SoMachine Motion Tools V4.3, SoMachine Software
SoMove, SoSafe Configurable, SoSafe Programmable V2.1
TeSysDTM
Unity Loader
Unity Pro
Vijeo Citect, Vijeo Designer, Vijeo Designer Opti 6.1, Vijeo XD
Web Gate
Client Files

Následky

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

Odporúčania
Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje
https://ics-cert.us-cert.gov/advisories/ICSA-18-305-02 https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-298-01+Schneider+Electric+Software+Update+%28SESU%29.pdf&p_Doc_Ref=SEVD-2018-298-01

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

Identifikátor

Red Hat Ansible zraniteľnosť

Popis

Vývojári zo spoločnosti Red Hat vydali aktualizáciu svojho produktu Red Hat Ansible, ktorá rieši bezpečnostnú zraniteľnosť v module User.
Lokálny autentifikovaný útočník by mohol túto zraniteľnosť zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

05.11.2018

CVE

CVE-2018-16837

Zasiahnuté systémy

Red Hat Ansible verzie staršie ako 2.7.1; 2.6.7; 2.5.11

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59097

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

Identifikátor

Fr. Sauter AG CASE Suite zraniteľnosť

Popis

Spoločnosť Fr. Sauter AG vydala bezpečnostnú aktualizáciu na svoj produkt CASE Suite, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

01.11.2018

CVE

CVE-2018-17912

Zasiahnuté systémy

CASE Suite verzie staršie ako 3.10 Service Release 1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-305-04

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

Identifikátor

F5 BIG-IP zraniteľnosti

Popis

Spoločnosť F5 vydala bezpečnostnú aktualizáciu na svoj produkt BIG-IP, ktorá opravuje bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené chybami v konfigurácií systému, ktoré by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

31.10.2018

CVE

CVE-2018-15317, CVE-2018-15318, CVE-2018-15319, CVE-2018-15320

Zasiahnuté systémy

BIG-IP verzie 14.x staršie ako 14.0.0.3
BIG-IP verzie 13.x staršie ako 13.1.1.2
BIG-IP verzie 12.x staršie ako 12.1.3.7
BIG-IP verzie 11.x staršie ako 11.6.3.3 a 11.5.7

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/152450
https://exchange.xforce.ibmcloud.com/vulnerabilities/152449
https://exchange.xforce.ibmcloud.com/vulnerabilities/152448
https://exchange.xforce.ibmcloud.com/vulnerabilities/152447

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Robotic Process Automation with Automation Anywhere zraniteľnosti

Popis

Vývojári spoločnosti IBM vydali aktualizáciu svojich produktov IBM Robotic, ktoré riešia viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v chýbajúcom šifrovaní citlivých autentifikačných údajov a lokálny neautentifikovaný útočník ju môže zneužiť vo na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

30.10.2018

CVE

CVE-2018-1876, CVE-2018-1877, CVE-2018-1878

Zasiahnuté systémy

IBM Robotic Process Automation with Automation Anywhere verzie staršie ako 11.0.0.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10735967
https://exchange.xforce.ibmcloud.com/vulnerabilities/151707
https://www-01.ibm.com/support/docview.wss?uid=ibm10735973
https://exchange.xforce.ibmcloud.com/vulnerabilities/151713
https://www-01.ibm.com/support/docview.wss?uid=ibm10735977
https://exchange.xforce.ibmcloud.com/vulnerabilities/151714

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

Identifikátor

GNOME gThumb zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v produkte GNOME gThumb.
Bezpečnostná zraniteľnosť umožňuje lokálnemu autentifikovanému útočníkovi prostredníctvom opakovaného volania funkcie g_free spôsobiť zneprístupnenie služby na napadnutom systéme.

Dátum prvého zverejnenia varovania

30.10.2018

CVE

CVE-2018-18718

Zasiahnuté systémy

gthumb verzie 2.7 až 3.6

Následky

Zneprístupnenie služby

Odporúčania

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

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=59070

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 4.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti v implementácii SSD hardvérového šifrovania TCG Opal SED

Popis

Bezpečnostní výskumníci informovali o zraniteľnostiach v implementácii štandardu TCG Opal pre hardvérové šifrovanie SSD diskov.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú útočníkovi s fyzickým prístupom ku zariadeniu získať neoprávnený prístup k citlivým údajom.
Konkrétny zdokumentovaný mechanizmus je nasledovný: šifrovanie disku nie je závislé od zadaného používateľského hesla, a tak je možné s prístupom k zasiahnutému SSD zmeniť heslo a následne získať plný prístup k údajom.

Dátum prvého zverejnenia varovania

05.11.2018

CVE

CVE-2018-12037, CVE-2018-12038

Zasiahnuté systémy

SSD disky:
Crucial (Micron) MX100, MX200, MX300
Samsung T3 a T5
Samsung 840 EVO a 850 EVO

Následky

Únik citlivých informácií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu firmvéru zasiahnutých SSD diskov.

Zdroje

https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2018-0984+1.00+Meerdere+kwetsbaarheden+ontdekt+in+implementaties+Self-Encrypting+Drives.html