BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 03. 2018 – 03. 04. 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-028

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

Identifikátor

Apple Releases Multiple Security Updates

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje produkty macOS, watchOS, tvOS, Safari, iTunes, iCloud a iOS, ktoré opravujú viacero bezpečnostných zraniteľností. Najvážnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných opatrení a umožňujú vzdialenému útočníkovi eskalovať svoje privilégiá na napadnutom systéme a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

29.03.2018

CVE

CVE-2017-13890, CVE-2017-8816, CVE-2018-4101, CVE-2018-4102, CVE-2018-4104 až CVE-2018-4108, CVE-2018-4110 až CVE-2018-4125, CVE-2018-4127 až CVE-2018-4140, CVE-2018-4142 až CVE-2018-4144, CVE-2018-4146, CVE-2018-4148 až CVE-2018-4152, CVE-2018-4154 až CVE-2018-4158, CVE-2018-4160 až CVE-2018-4168, CVE-2018-4170, CVE-2018-4172, CVE-2018-4174, CVE-2018-4175, CVE-2018-4176

Zasiahnuté systémy

watchOS, Xcode, tvOS, Safari, iTunes, iCloud, iOS
macOS High Sierra, macOS Sierra, macOS El Capitan

Následky

Vykonanie škodlivého kódu, Zneprístupnenie služby, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom, Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT208693
https://support.apple.com/en-us/HT208697
https://support.apple.com/en-us/HT208694
https://support.apple.com/en-us/HT208692
https://support.apple.com/en-us/HT208695
https://support.apple.com/en-us/HT208698
https://support.apple.com/en-us/HT208696
https://support.apple.com/en-us/HT208699

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

Identifikátor

Microsoft Release Patch for Windows 7 and Windows Server 2008 R2 Systems

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje operačné systémy Windows 7 a Windows Server 2008 R2, ktoré opravujú bezpečnostnú zraniteľnosť v zabezpečení systémového jadra.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

29.03.2018

CVE

CVE-2018-1038

Zasiahnuté systémy

Windows 7 for x64-based Systems SP1
Windows Server 2008 R2 for x64-based Systems SP1

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.kb.cert.org/vuls/id/277400
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1038

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

Identifikátor

RSA Authentication Agent for Web Multiple Vulnerabilities

Popis

Produkt RSA Authentication Agent for Web pre IIS a Apache Web Server obsahuje viacero zraniteľností.
Najzávažnejšia zraniteľnosť spočíva v nesprávnom spracovávaní cookies a vzdialený neautentifkovaný útočník by ju mohol prostredníctvom podvrhnutia cookies so špecifickou hodnotou zneužiť na zneprístupnenie služby.
Ďalšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý JavacSript kód v kontexte stránky využívajúcej RSA Authentication Agent.
Posledná zraniteľnosť spočíva v nesprávnej implementácii zoznamu pre riadenie prístupov ACL a lokálny útočník by ju mohol zneužiť na prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.03.2018

CVE

CVE-2018-1232, CVE-2018-1233, CVE-2018-1234

Zasiahnuté systémy

RSA Authentication Agent for Web for IIS verzie 8.0.1 a staršie
RSA Authentication Agent for Web for Apache Web Server verzie 8.0.1 a staršie (len CVE-2018-1232, CVE-2018-1233)

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://securitytracker.com/id/1040577
http://seclists.org/fulldisclosure/2018/Mar/60

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

Identifikátor

Apache Software Foundation Releases Security Update

Popis

Vývojári nástroja Apache Sturts vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v plugine REST.
Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne upravených XML súborov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

31.03.2018

CVE

CVE-2018-1327

Zasiahnuté systémy

Struts 2.1.1 - Struts 2.5.14.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://cwiki.apache.org/confluence/display/WW/S2-056
https://access.redhat.com/security/cve/cve-2018-1327

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

Identifikátor

OpenSSL Security Bypass Vulnerabilities

Popis

Vývojári OpenSSL vydali aktualizáciu svojho produktu, ktorá rieši viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služieb na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

27.03.2018

CVE

CVE-2017-3738, CVE-2018-0733, CVE-2018-0739

Zasiahnuté systémy

OpenSSL 1.1.0
OpenSSL 1.0.2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.openssl.org/news/secadv/20180327.txt

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell EMC ScaleIO Multiple Vulnerabilities

Popis

Spoločnosť Dell EMC vydala bezpečnostnú aktualizáciu, ktorá opravuje viacero zraniteľností v produkte Dell EMC ScaleIO.
Najzávažnejšia je zraniteľnosť nachádzajúca sa v komponente LIA (Light Installation Agent), ktorú by vzdialený útočník s administrátorským heslom k LIA mohol zneužiť na vykonanie príkazov s oprávneniami úrovne root v systéme, na ktorom je zraniteľný komponent nainštalovaný.
Ďalšia zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie v komponente LIA a vzdialený neautentifikovaný útočník by ju mohol zneužiť na realizáciu brute-force útokov na používateľské účty LIA.

Dátum prvého zverejnenia varovania

26.03.2018

CVE

CVE-2018-1205, CVE-2018-1237, CVE-2018-1238

Zasiahnuté systémy

Dell EMC ScaleIO verzie staršej ako 2.5

Následky

Neoprávnený prístup do systému, Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://seclists.org/fulldisclosure/2018/Mar/59

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

Identifikátor

Schneider Electric Modicon FTP Vulnerabilities

Popis

Spoločnosť Schneider Electric informuje používateľov svojich produktov Modicon o viacerých bezpečnostných zraniteľnostiach v FTP funkciách v ich komunikačných moduloch.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému autentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme a tiež vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

22.03.2018 (aktualizácia 30.03.2018)

CVE

CVE-2018-7240, CVE-2018-7241, CVE-2018-7242

Zasiahnuté systémy

Modicon Premium, Modicon Quantum, Modicon M340, Modicon X80 RTU

Následky

Neoprávnená zmena v systéme, Vykonanie škodlivého kódu

Odporúčania

Spoločnosť Schneider Electric dosiaľ neuviedla, či vydá aktualizácie riešiace uvedené zraniteľnosti. Administrátorom zasiahnutých systémov odporúčame aplikovať firewallové pravidlá a limitovať sieťový prístup k zasiahnutým zariadeniam. Taktiež odporúčame vypnúť na zasiahnutých zariadeniach podporu FTP a zapínať ju iba v prípade aktualizácie a konfigurácie systémov.

Zdroje

https://www.schneider-electric.com/en/download/document/SEVD-2018-081-01/
https://ics-cert.us-cert.gov/advisories/ICSA-18-086-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.4
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

QNAP QTS Multiple Vulnerabilities

Popis

Spoločnosť QNAP vydala aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v produkte QTS.
Najzávažnejšie zraniteľnosti v module File Station by vzdialený neautentifikovaný útočník mohol zneužiť na realizáciu XSS (Cross-Site Scripting) útoku a v prípade jeho úspešnosti vykonať škodlivý webový skript.
Ďalšiu zraniteľnosť by vzdialený neautentifikovaný útočník mohol prostredníctvom požiadavky na sysinfoReq.cgi zneužiť na získanie prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

23.03.2018 (posledná aktualizácia 27.03.2018)

CVE

CVE-2017-7629, CVE-2017-7630, CVE-2017-7631, CVE-2017-7632

Zasiahnuté systémy

QNAP QTS 4.2.6: build 20171026 a staršie verzie
QNAP QTS 4.3.3: build 20170727 a staršie verzie

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.qnap.com/zh-tw/security-advisory/nas-201803-23

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

Identifikátor

Philips Alice 6 Vulnerabilities

Popis

Spoločnosť Philips vydala bezpečnostnú aktualizáciu na svoj produkt Philips Alice 6, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných opatrení a umožňujú vzdialenému neautentifikovanému útočníkovi získať prístup k citlivým údajom používateľov.

Dátum prvého zverejnenia varovania

27.03.2018

CVE

CVE-2018-5451, CVE-2018-7498

Zasiahnuté systémy

Philips Alice 6 verzie staršie ako R8.0.3

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov a obmedziť sieťový prístup ku zariadeniam v súlade s používateľským manuálom.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSMA-18-086-01