BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 05. 2020 - 26. 05. 2020

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:
01439/2020/SK-CERT-125

BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 05. 2020 - 26. 05. 2020

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

Identifikátor

VMware Cloud Director zraniteľnosť

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt Cloud Director, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.05.2020

CVE

CVE-2020-3956

Zasiahnuté systémy

VMware Cloud Director verzie staršie ako 10.1.0, 10.0.0.2, 9.7.0.5, 9.5.0.6 a 9.1.0.4

Následky

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

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2020-0010.html

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:
01439/2020/SK-CERT-125

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

Identifikátor

Adobe produkty viacero zraniteľností

Popis

Spoločnosť Adobe vydala aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť v produkte Character Animator je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.05.2020

CVE

CVE-2020-9586, CVE-2020-9616, CVE-2020-9617, CVE-2020-9618

Zasiahnuté systémy

Adobe Premiere Rush verzie staršie ako 1.5.12
Adobe Audition verzie staršie ako 13.0.6
Adobe Premiere Pro verzie staršie ako 14.2
Adobe Character Animator 2020 verzie staršie ako 3.3

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://helpx.adobe.com/security/products/premiere_rush/apsb20-29.html
https://helpx.adobe.com/security/products/audition/apsb20-28.html
https://helpx.adobe.com/security/products/premiere_pro/apsb20-27.html
https://helpx.adobe.com/security/products/character_animator/apsb20-25.html
https://threatpost.com/adobe-patches-critical-rce-flaw-character-animator/155882/

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

Identifikátor

Google Chrome viacero zraniteľností

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.05.2020

CVE

CVE-2020-6465, CVE-2020-6466, CVE-2020-6467, CVE-2020-6468, CVE-2020-6469, CVE-2020-6470, CVE-2020-6471, CVE-2020-6472, CVE-2020-6473, CVE-2020-6474, CVE-2020-6475, CVE-2020-6476, CVE-2020-6477, CVE-2020-6478, CVE-2020-6479, CVE-2020-6480, CVE-2020-6481, CVE-2020-6482, CVE-2020-6483, CVE-2020-6484, CVE-2020-6485, CVE-2020-6486, CVE-2020-6487, CVE-2020-6488, CVE-2020-6489, CVE-2020-6490, CVE-2020-6491

Zasiahnuté systémy

Google Chrome verzie staršie ako 83.0.4103.61

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2020-069/

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

Identifikátor

Zraniteľnosti produktov Rockwell Automation

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti v komponente EDS Subsystem sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

19.05.2020

CVE

CVE-2020-12034, CVE-2020-12038

Zasiahnuté systémy

EDS Subsystem verzia 28.0.1 a staršie
FactoryTalk Linx software verzie 6.00, 6.10, a 6.11
RSLinx Classic: verzia 4.11.00 a staršie
RSNetWorx software: verzia 28.00.00 a staršie
Studio 5000 Logix Designer software: verzia 32 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a blokovať porty TCP 2222, 7153 a UDP 44818.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-20-140-01

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

Identifikátor

Schneider Electric EcoStruxure Operator Terminal Expert viacero zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt EcoStruxure Operator Terminal Expert, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.05.2020

CVE

CVE-2020-7493, CVE-2020-7494, CVE-2020-7495, CVE-2020-7496, CVE-2020-7497

Zasiahnuté systémy

Schneider Electric EcoStruxure™ Operator Terminal Expert verzie staršie ako 3.1 Service Pack 1A

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2020-133-04_EcoStruxure%E2%84%A2+Operator+Terminal+Expert_Security_Notification.pdf&p_Doc_Ref=SEVD-2020-133-04
https://www.us-cert.gov/ics/advisories/icsa-20-142-02

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

Identifikátor

Emerson OpenEnterprise SCADA zraniteľnosti

Popis

Spoločnosť Emerson vydala aktualizáciu na svoj produkt OpenEnterprise, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii autentifikačných mechanizmov umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.05.2020

CVE

CVE-2020-10632, CVE-2020-10636, CVE-2020-10640

Zasiahnuté systémy

Emerson OpenEnterprise verzie staršie ako 3.3.5

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-20-140-02

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

Identifikátor

ABB Device Library Wizard zraniteľnosť

Popis

Spoločnosť ABB vydala bezpečnostnú aktualizáciu na svoj produkt Device Library Wizard, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

14.05.2020

CVE

CVE-2020-8482

Zasiahnuté systémy

ABB Device Library Wizard verzie staršie ako 6.0.3.2RU1, 6.0.3.3 a 6.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

http://search.abb.com/library/Download.aspx?DocumentID=3ADR010466&LanguageCode=en&DocumentPartId=&Action=Launch

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Drupal CMS viacero zraniteľností

Popis

Vývojári redakčného systému Drupal vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

20.05.2020

CVE

CVE-2020-11022, CVE-2020-11023

Zasiahnuté systémy

Drupal verzie staršie ako 8.8.6, 8.7.14. a 7.7

Následky

Neoprávnená zmena v systéme
Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Drupal v zraniteľných verziách. V prípade že áno, zabezpečte aktualizáciu redakčného systému a zásuvných modulov.
Po odstránení zraniteľností, ktoré môžu spôsobiť únik informácií, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.drupal.org/sa-core-2020-002
https://www.drupal.org/sa-core-2020-003
https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2
https://github.com/jquery/jquery/security/advisories/GHSA-jpcq-cgw6-v4j6
https://exchange.xforce.ibmcloud.com/vulnerabilities/182278
https://exchange.xforce.ibmcloud.com/vulnerabilities/182277