BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 06. 2020 - 30. 06. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Bitdefender Total Security 2020 - zraniteľnosť	Vysoká	**8.8**
02.	Mattermost - viacero zraniteľností	Vysoká	**8.8**
03.	Adobe Magento - viacero zraniteľností	Vysoká	**8.8**
04.	Google Chrome - viacero zraniteľností	Vysoká	**8.8**
05.	Rockwell Automation FactoryTalk - zraniteľnosti	Vysoká	**8.8**
06.	DrayTek Vigor - zraniteľnosti	Vysoká	**8.8**
07.	NVIDIA GPU Display Driver - zraniteľnosti	Vysoká	**7.8**
08.	Apache Tomcat - zraniteľnosť	Vysoká	**7.5**

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-165

BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 06. 2020 - 30. 06. 2020

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

Identifikátor

Bitdefender Total Security 2020 - zraniteľnosť

Popis

Spoločnosť Bitdefender vydala aktualizáciu na svoj produkt Bitdefender Total Security 2020, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v komponente SafePay 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

22.06.2020

CVE

CVE-2020-8102

Zasiahnuté systémy

Bitdefender Total Security 2020 verzie staršie ako 24.0.20.116

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://www.bitdefender.com/support/security-advisories/insufficient-url-sanitization-validation-safepay-browser-va-8631/
https://exchange.xforce.ibmcloud.com/vulnerabilities/183890
https://www.cisecurity.org/advisory/a-vulnerability-in-bitdefender-safepay-could-allow-for-remote-code-execution_2020-085/

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

Identifikátor

Mattermost - viacero zraniteľností

Popis

Vývojári komunikačného nástroja Mattermost vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať prístup k citlivým údajom a tiež spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

19.06.2020

CVE

CVE-2020-14447, CVE-2020-14448, CVE-2020-14449, CVE-2020-14450, CVE-2020-14451, CVE-2020-14452, CVE-2020-14453, CVE-2020-14454, CVE-2020-14455, CVE-2020-14456, CVE-2020-14457, CVE-2020-14458, CVE-2020-14459, CVE-2020-14460

Zasiahnuté systémy

Mattermost Server verzie staršie ako 5.24.0
Mattermost Mobile Apps verzie staršie ako 1.31.2

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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://exchange.xforce.ibmcloud.com/vulnerabilities/183714
https://exchange.xforce.ibmcloud.com/vulnerabilities/183713
https://exchange.xforce.ibmcloud.com/vulnerabilities/183712
https://exchange.xforce.ibmcloud.com/vulnerabilities/183711
https://exchange.xforce.ibmcloud.com/vulnerabilities/183708
https://exchange.xforce.ibmcloud.com/vulnerabilities/183707
https://exchange.xforce.ibmcloud.com/vulnerabilities/183706
https://exchange.xforce.ibmcloud.com/vulnerabilities/183705
https://exchange.xforce.ibmcloud.com/vulnerabilities/183704
https://exchange.xforce.ibmcloud.com/vulnerabilities/183703
https://exchange.xforce.ibmcloud.com/vulnerabilities/183702
https://exchange.xforce.ibmcloud.com/vulnerabilities/183701

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

Identifikátor

Adobe Magento - viacero zraniteľností

Popis

Vývojári E-commerce platformy Magento vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť 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

22.06.2020

CVE

CVE-2020-9664, CVE-2020-9665

Zasiahnuté systémy

Magento Commerce 1 verzie staršie ako SUPEE-11346
Magento Open Source 1 verzie staršie ako SUPEE-11346

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Magento v zraniteľnej verzii. V prípade že áno, zabezpečte aktualizáciu redakčného systému a pluginov.
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/magento/apsb20-41.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/183853
https://exchange.xforce.ibmcloud.com/vulnerabilities/183852

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

22.06.2020

CVE

CVE-2020-6509

Zasiahnuté systémy

Google Chrome verzie staršie ako 83.0.4103.116

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://www.cisecurity.org/advisory/a-vulnerability-in-google-chrome-could-allow-for-arbitrary-code-execution_2020-084/
https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-desktop_22.html
https://access.redhat.com/security/cve/CVE-2020-6509

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

Identifikátor

Rockwell Automation FactoryTalk - zraniteľnosti

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoj produkt FactoryTalk, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a do systému.

Dátum prvého zverejnenia varovania

25.06.2020

CVE

CVE-2020-14478, CVE-2020-14480, CVE-2020-14481

Zasiahnuté systémy

Rockwell Automation FactoryTalk View SE verzie staršie ako 10.0
Rockwell Automation FactoryTalk Services Platform 6.11 Patch 1066644

Následky

Neoprávnený prístup k citlivým údajom
Eskalácia privilégií
Neoprávnený prístup do systému

Odporúčania

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

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-20-177-03
https://www.us-cert.gov/ics/advisories/icsa-20-177-02

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

Identifikátor

DrayTek Vigor - zraniteľnosti

Popis

Spoločnosť DrayTek vydala bezpečnostnú aktualizáciu na svoje smerovače Vigor 2960, 3900, 300B, ktorá opravuje viacero bezpečnostných zraniteľností.
Bližšie nešpecifikované bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.06.2020

CVE

CVE-2020-14472, CVE-2020-14473, CVE-2020-14993

Zasiahnuté systémy

DrayTek Vigor 2960, 3900, 300B firmvér verzie staršie ako 1.5.1.1

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)
https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-remote-code-injection/execution-vulnerability-(cve-2020-14472)
https://github.com/dexterone/Vigor-poc
https://nvd.nist.gov/vuln/detail/CVE-2020-14472
https://nvd.nist.gov/vuln/detail/CVE-2020-14473
https://nvd.nist.gov/vuln/detail/CVE-2020-14993

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

Identifikátor

NVIDIA GPU Display Driver - zraniteľnosti

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje produkty GPU Display Driver a Virtual GPU Manager, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.06.2020

CVE

CVE-2020-5962, CVE-2020-5963, CVE-2020-5964, CVE-2020-5965, CVE-2020-5966, CVE-2020-5967, CVE-2020-5968, CVE-2020-5969, CVE-2020-5970, CVE-2020-5971, CVE-2020-5972, CVE-2020-5973

Zasiahnuté systémy

NVIDIA GPU Display Driver verzie staršie ako 451.48, 443.18, 426.78, 392.61, 443.18, 426.78, 450.51, 440.100, 390.138, 440.95.01 a 418.152.00
NVIDIA vGPU Software verzie staršie ako 432.44, 426.72, 430.99, 418.149

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5031
https://nvd.nist.gov/vuln/detail/CVE-2020-5965
https://nvd.nist.gov/vuln/detail/CVE-2020-5964
https://nvd.nist.gov/vuln/detail/CVE-2020-5963

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

Identifikátor

Apache Tomcat - zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoj produkt Tomcat, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených HTTP/2 požiadaviek spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

25.06.2020

CVE

CVE-2020-11996

Zasiahnuté systémy

Apache Tomcat verzie staršie ako 10.0.0-M6, 9.0.36, 8.5.56

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie.

Zdroje

http://mail-archives.us.apache.org/mod_mbox/www-announce/202006.mbox/%3Cfd56bc1d-1219-605b-99c7-946bf7bd8ad4%40apache.org%3E
https://nvd.nist.gov/vuln/detail/CVE-2020-11996
https://access.redhat.com/security/cve/cve-2020-11996