BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 10. 2020 - 20. 10. 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-255

BEZPEČNOSTNÝ BULLETIN

Týždeň 14. 10. 2020 - 20. 10. 2020

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

Identifikátor

Adobe Flash Player - zraniteľnosť

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Adobe Flash Player, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.10.2020

CVE

CVE-2020-9746

Zasiahnuté systémy

Adobe Flash Player Desktop Runtime pre Windows a macOS verzie staršie ako 32.0.0.433
Adobe Flash Player Desktop Runtime pre Linux verzie staršie ako 32.0.0.433
Adobe Flash Player pre Google Chrome pre Windows, macOS, Linux a Chrome OS verzie staršie ako 32.0.0.433
Adobe Flash Player pre Microsoft Edge a Internet Explorer 11 pre Windows 10 a 8.1 verzie staršie ako 32.0.0.387

Následky

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

Odporúčania

Administrátorom a používateľom 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://helpx.adobe.com/security/products/flash-player/apsb20-58.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9746
https://securityaffairs.co/wordpress/109448/hacking/adobe-flash-player-critical-flaw.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-255

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

Identifikátor

Apache Hadoop - zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoj produkt Apache Hadoop, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a vzdialený autentifikovaný útočník by ju prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek mohol zneužiť na eskaláciu privilégií v systéme a vydávať sa za ľubovoľného používateľa systému.

Dátum prvého zverejnenia varovania

21.10.2020

CVE

CVE-2018-11764

Zasiahnuté systémy

Apache Hadoop verzie 3.0.0-beta1
Apache Hadoop verzie 3.0.0-alpha4
Apache Hadoop verzie 3.0.0

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli viesť k úniku citlivých údajov, 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://seclists.org/oss-sec/2020/q4/80
https://exchange.xforce.ibmcloud.com/vulnerabilities/190362

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

Identifikátor

Google Chrome - aktualizácia

Popis

Spoločnosť Google vydala bezpečnostné aktualizácie na svoj internetový prehliadač Chrome, ktorý opravuje viacero bezpečnostných zraniteľností a chýb.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.10.2020

CVE

CVE-2020-15999, CVE-2020-16000, CVE-2020-16001, CVE-2020-16002, CVE-2020-16003

Zasiahnuté systémy

Google Chrome verzie staršie ako 86.0.4240.111

Následky

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

Odporúčania

Administrátorom a používateľom 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/2020/10/stable-channel-update-for-desktop_20.html
https://thehackernews.com/2020/10/chrome-zeroday-attacks.html

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

Identifikátor

Mozilla Firefox - bezpečnostné zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností vo webovom prehliadači Firefox.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.10.2020

CVE

CVE-2020-15254, CVE-2020-15680, CVE-2020-15681, CVE-2020-15682, CVE-2020-15683, CVE-2020-15684, CVE-2020-15969

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 81
Mozilla Firefox ESR verzie staršie ako 78.3

Následky

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

Odporúčania

Administrátorom a používateľom 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.mozilla.org/en-US/security/advisories/mfsa2020-45/

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 bezpečnostné aktualizácie na portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.10.2020

CVE

CVE-2020-24409, CVE-2020-24410, CVE-2020-24411, CVE-2020-24412, CVE-2020-24413, CVE-2020-24414, CVE-2020-24415, CVE-2020-24416, CVE-2020-24418, CVE-2020-24419, CVE-2020-24420, CVE-2020-24421, CVE-2020-24422, CVE-2020-24423, CVE-2020-24424, CVE-2020-24425, CVE-2020-9747, CVE-2020-9748, CVE-2020-9749, CVE-2020-9750

Zasiahnuté systémy

Illustrator 2020 verzie 24.2 a staršie
Adobe Dreamweaver verzie 20.2 a staršie
Marketo Sales Insight Salesforce verzie package 1.4355 a staršie
Animate verzie 20.5 a staršie
Adobe After Effects verzie 17.1.1 a staršie
Photoshop CC 2019 verzie 20.0.10 a staršie
Photoshop 2020 verzie 21.2.2 a staršie
Adobe Premiere Pro verzie 14.4 a staršie
Adobe Media Encoder verzie 14.4 a staršie
Adobe InDesign verzie 15.1.2 a staršie
Creative Cloud Desktop Application verzie 5.2 a staršie
Creative Cloud Desktop Application verzie 2.1 a staršie

Následky

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

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/illustrator/apsb20-53.html
https://helpx.adobe.com/security/products/dreamweaver/apsb20-55.html
https://helpx.adobe.com/security/products/marketo/apsb20-60.html
https://helpx.adobe.com/security/products/animate/apsb20-61.html
https://helpx.adobe.com/security/products/after_effects/apsb20-62.html
https://helpx.adobe.com/security/products/photoshop/apsb20-63.html
https://helpx.adobe.com/security/products/premiere_pro/apsb20-64.html
https://helpx.adobe.com/security/products/media-encoder/apsb20-65.html
https://helpx.adobe.com/security/products/indesign/apsb20-66.html
https://helpx.adobe.com/security/products/creative-cloud/apsb20-68.html

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

Identifikátor

Cisco produkty - viacero zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty Cisco ASA (Adaptive Security Appliance), FMC (Firepower Management Center), and FTD (Firepower Threat Defense) Software, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na získanie neoprávneného prístupu do systému alebo zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.10.2020

CVE

CVE-2020-3304, CVE-2020-3373, CVE-2020-3410, CVE-2020-3436, CVE-2020-3499, CVE-2020-3514, CVE-2020-3528, CVE-2020-3529, CVE-2020-3533, CVE-2020-3549, CVE-2020-3550, CVE-2020-3554, CVE-2020-3562, CVE-2020-3563, CVE-2020-3571, CVE-2020-3572, CVE-2020-3577

Zasiahnuté systémy

Cisco Adaptive Security Appliance
Cisco Firepower Management Center
Cisco Firepower Threat Defense
Konkrétne verzie zasiahnutých produktov sú špecifikované na:
https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-74302

Následky

Zneprístupnenie služby
Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu systémov.
Po odstránení zraniteľností, ktoré mohli viesť k úniku citlivých údajov, 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://tools.cisco.com/security/center/viewErp.x?alertId=ERP-74302
https://www.securityweek.com/cisco-patches-17-high-severity-vulnerabilities-security-appliances
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-QFcNEPfx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-frag-memleak-mCtqdP9n
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ospflls-37Xy2q6r
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-sslvpndma-dos-HRrqB9Yx
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-tcp-dos-N3DMnU4T
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webdos-fBzM5Ynw
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-fileup-dos-zvC7wtys
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-ssl-dcrpt-dos-RYEkX4yy
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-icmp-dos-hxxcycM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdfmc-dirtrav-NW8XcuSB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdfmc-sft-mitm-tc8AzFs2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cacauthbyp-NCLGZm3Q
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdfmc-dos-NjYvDcLA
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-inline-dos-nXqUyEqM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-container-esc-FmYqFBQV
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snmp-dos-R8ENPbOs
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tcp-dos-GDcZDqAf

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

Identifikátor

Linux BlueZ Bluetooth Stack - zraniteľnosti BleedingTooth

Popis

Bezpečnostní výskumníci zverejnili informácie o trojici zraniteľností v open-source implementácii Bluetooth stacku BlueZ, ktoré sú súhrnne označované ako BleedingTooth.
Najzávažnejšie zraniteľnosti by neautentifikovaný útočník v dosahu Bluetooth komunikácie mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.10.2020

CVE

CVE-2020-12351, CVE-2020-12352, CVE-2020-24490

Zasiahnuté systémy

Všetky verzie Linux kernelov podporujúcich BlueZ

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
Neoprávený 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://thehackernews.com/2020/10/linux-Bluetooth-hacking.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html

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

Identifikátor

Allen-Bradley 1794-AENT Flex I/O series B - viacero zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostných zraniteľnostiach v produktoch Allen-Bradley 1794-AENT Flex I/O series B.
Zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom zasielania špeciálne vytvorených paketov mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

14.10.2020

CVE

CVE-2020-6084, CVE-2020-6085, CVE-2020-6086, CVE-2020-6087, CVE-2020-6088

Zasiahnuté systémy

Allen-Bradley 1794-AENT Flex I/O series B adaptéri verzie 4.003 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Spoločnosť Rockwell Automation odporúča limitovanie CIP spojení na porte 44818 len na spojenia z dôveryhodných zdrojov, zavedenie segmentácie siete a firewallových pravidiel limitujúcich prístup k daným zariadeniam.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

Zdroje

https://www.securityweek.com/remotely-exploitable-dos-vulnerabilities-found-allen-bradley-adapter
https://blog.talosintelligence.com/2020/10/vuln-spotlight-allen-bradley-dos-flex-io.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Magento - viacero zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na e-commerce platformu Magento, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený autentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.10.2020

CVE

CVE-2020-24400, CVE-2020-24401, CVE-2020-24402, CVE-2020-24403, CVE-2020-24404, CVE-2020-24405, CVE-2020-24406, CVE-2020-24407, CVE-2020-24408

Zasiahnuté systémy

Magento Commerce verzie 2.3.5-p1 a staršie
Magento Commerce verzie 2.3.5-p2 a staršie
Magento Commerce verzie 2.4.0 a staršie
Magento Open Source verzie 2.3.5-p1 a staršie
Magento Open Source verzie 2.3.5-p2 a staršie
Magento Open Source verzie 2.4.0 a staršie

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://www.zdnet.com/article/adobe-patches-magento-bugs-that-lead-to-code-execution-customer-list-tampering/
https://helpx.adobe.com/security/products/magento/apsb20-59.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BigBlueButton - zraniteľnosť

Popis

Vývojári webovej komunikačnej platformy BigBlueButton vydali bezpečnostnú aktualizáciu, ktorá odstraňuje bezpečnostnú zraniteľnosť.
Bezpečnostnú zraniteľnosť by vzdialený autentifikovaný útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom a na realizáciu SSRF útokov.
Na uvedenú zraniteľnosť je dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

21.10.2020

CVE

CVE-2020-25820

Zasiahnuté systémy

BigBlueButton verzie 2.2.25

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli viesť k úniku citlivých údajov, 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://packetstormsecurity.com/files/159667
https://seclists.org/fulldisclosure/2020/Oct/26

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-255