BEZPEČNOSTNÝ BULLETIN

Týždeň 15. 04. 2020 - 21. 04. 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-093

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

Identifikátor

Google Chrome zraniteľnosť

Popis

Spoločnosť Google vydala aktualizáciu na svoj internetový prehliadač Google Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v komponente speech recognizer umožňuje 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

15.04.2020

CVE

CVE-2020-6457

Zasiahnuté systémy

Google Chrome verzie staršie ako 81.0.4044.113

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/2020/04/stable-channel-update-for-desktop_15.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/179626

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

Identifikátor

Foxit Reader a PhantomPDF zraniteľnosti

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoje produkty Foxit Reader a PhantomPDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.04.2020

CVE

CVE-2020-10889, CVE-2020-10890, CVE-2020-10891, CVE-2020-10892, CVE-2020-10893, CVE-2020-10894, CVE-2020-10895, CVE-2020-10896, CVE-2020-10897, CVE-2020-10898, CVE-2020-10899, CVE-2020-10900, CVE-2020-10901, CVE-2020-10902, CVE-2020-10903, CVE-2020-10904, CVE-2020-10905, CVE-2020-10906, CVE-2020-10907, CVE-2020-10908, CVE-2020-10909, CVE-2020-10910, CVE-2020-10911, CVE-2020-10912, CVE-2020-10913

Zasiahnuté systémy

Foxit Reader verzie staršie ako 9.7.2
Foxit PhantomPDF verzie staršie ako 9.7.2

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 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.foxitsoftware.com/support/security-bulletins.php
https://www.zerodayinitiative.com/advisories/ZDI-20-535/
https://www.zerodayinitiative.com/advisories/ZDI-20-516/
https://www.zerodayinitiative.com/advisories/ZDI-20-511/
https://www.zerodayinitiative.com/advisories/ZDI-20-515/
https://www.zerodayinitiative.com/advisories/ZDI-20-513/
https://www.zerodayinitiative.com/advisories/ZDI-20-512/
https://www.zerodayinitiative.com/advisories/ZDI-20-514/
https://www.zerodayinitiative.com/advisories/ZDI-20-517/
https://www.zerodayinitiative.com/advisories/ZDI-20-530/
https://www.zerodayinitiative.com/advisories/ZDI-20-520/
https://www.zerodayinitiative.com/advisories/ZDI-20-518/
https://www.zerodayinitiative.com/advisories/ZDI-20-519/
https://www.zerodayinitiative.com/advisories/ZDI-20-521/
https://www.zerodayinitiative.com/advisories/ZDI-20-534/
https://www.zerodayinitiative.com/advisories/ZDI-20-522/
https://www.zerodayinitiative.com/advisories/ZDI-20-523/
https://www.zerodayinitiative.com/advisories/ZDI-20-524/
https://www.zerodayinitiative.com/advisories/ZDI-20-525/
https://www.zerodayinitiative.com/advisories/ZDI-20-533/
https://www.zerodayinitiative.com/advisories/ZDI-20-526/
https://www.zerodayinitiative.com/advisories/ZDI-20-528/
https://www.zerodayinitiative.com/advisories/ZDI-20-529/
https://www.zerodayinitiative.com/advisories/ZDI-20-527/
https://www.zerodayinitiative.com/advisories/ZDI-20-532/
https://www.zerodayinitiative.com/advisories/ZDI-20-531/

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

Identifikátor

Jenkins plugins viacero zraniteľností

Popis

Vývojári produktu Jenkins informovali o bezpečnostných zraniteľnostiach vo viacerých zásuvných moduloch.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.04.2020

CVE

CVE-2020-2177, CVE-2020-2178, CVE-2020-2179, CVE-2020-2180

Zasiahnuté systémy

AWS SAM Plugin verzie staršie ako 1.2.3
Copr Plugin verzie staršie ako 0.6.1
Parasoft Findings Plugin verzie staršie ako 10.4.4
Yaml Axis Plugin verzie staršie ako 0.2.1

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://jenkins.io/security/advisory/2020-04-16/
https://exchange.xforce.ibmcloud.com/vulnerabilities/179923
https://exchange.xforce.ibmcloud.com/vulnerabilities/179924
https://exchange.xforce.ibmcloud.com/vulnerabilities/179922
https://exchange.xforce.ibmcloud.com/vulnerabilities/179921

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

Identifikátor

Amazon Echo Show zraniteľnosť

Popis

Spoločnosť Amazon vydala aktualizáciu na svoje produkty Echo Show, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

15.04.2020

CVE

-

Zasiahnuté systémy

Amazon Echo Show verzie staršie ako 3523856004

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.zerodayinitiative.com/advisories/ZDI-20-537/
https://exchange.xforce.ibmcloud.com/vulnerabilities/179917

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

Identifikátor

WebKitGTK a WPE WebKit zraniteľnosť

Popis

Vývojári WebKitGTK a WPE WebKit vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje 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

16.04.2020

CVE

CVE-2020-11793

Zasiahnuté systémy

WebKitGTK a WPE WebKit verzie staršie ako 2.28.1.
GNOME aplikácie zobrazujúce webový obsah - webové prehliadače, e-mailoví klienti a iné

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://webkitgtk.org/security/WSA-2020-0004.html
https://wpewebkit.org/security/WSA-2020-0004.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/179915
https://seclists.org/oss-sec/2020/q2/34

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

Identifikátor

Micro Focus Enterprise Developer and Enterprise Server zraniteľnosť

Popis

Spoločnosť Micro Focus vydala bezpečnostnú aktualizáciu na svoj produkt Enterprise Server, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

16.04.2020

CVE

CVE-2020-9523

Zasiahnuté systémy

Micro Focus Enterprise Developer and Enterprise Server verzie staršie ako 4.0 Patch Update 16 a 5.0 Patch Update 6

Následky

Neoprávnený prístup k citlivým údajom

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://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03634936
https://exchange.xforce.ibmcloud.com/vulnerabilities/180037

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware vRealize Log Insight zraniteľnosti

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt vRealize Log Insight, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom XSS útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.04.2020

CVE

CVE-2020-3953, CVE-2020-3954

Zasiahnuté systémy

VMware vRealize Log Insight verzie staršie ako 8.1.0

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-2020-0007.html

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

Identifikátor

Intel produkty viacero zraniteľností

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť vo firmvéri Intel NUC umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

14.04.2020

CVE

CVE-2020-0547, CVE-2020-0557, CVE-2020-0558, CVE-2020-0568, CVE-2020-0576, CVE-2020-0577, CVE-2020-0578, CVE-2020-0598, CVE-2020-0600

Zasiahnuté systémy

Intel® NUC 8 Rugged Kit NUC8CCHKR
Intel® NUC Board NUC8CCHB
Intel® NUC 7 Essential PC NUC7CJYSAL
Intel® NUC Kit NUC7CJYH
Intel® NUC Kit NUC7PJYH
Intel® NUC Kit NUC6CAYS
Intel® NUC Kit NUC6CAYH
Intel® NUC Kit DE3815TYKHE
Intel® NUC Board DE3815TYBE
Intel® Compute Stick STCK1A32WFC
Intel® Binary Configuration Tool for Windows
Intel® Modular Server MFS2600KISPP Compute Module
Intel® Driver and Support Assistant verzie staršie ako 20.1.5
Intel® PROSet/Wireless WiFi verzie staršie ako 21.70
Intel® Data Migration Software

Následky

Eskalácia privilégií
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Produkty, ktorým bola ukončená technická podpora odporúčame odinštalovať zo systému.

Zdroje
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00363.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00359.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00338.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00327.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00344.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00351.html https://www.bleepingcomputer.com/news/security/intel-april-platform-update-fixes-high-severity-security-issues/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
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.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi eskalovať svoje privilégiá a získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

14.04.2020

CVE

CVE-2020-3767, CVE-2020-3768, CVE-2020-3796, CVE-2020-3798, CVE-2020-3809

Zasiahnuté systémy

Adobe Digital Editions verzie staršie ako 4.5.11.187303
Adobe After Effects verzie staršie ako 17.0.6
ColdFusion 2016 verzie staršie ako Update 15
ColdFusion 2018 verzie staršie ako Update 9

Následky

Zneprístupnenie služby
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

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://helpx.adobe.com/security/products/coldfusion/apsb20-18.html
https://helpx.adobe.com/security/products/after_effects/apsb20-21.html
https://helpx.adobe.com/security/products/Digital-Editions/apsb20-23.html
https://www.securityweek.com/adobe-patches-flaws-coldfusion-after-effects-digital-editions
https://threatpost.com/adobe-fixes-important-flaws-in-coldfusion-after-effects-and-digital-editions/154780/