BEZPEČNOSTNÝ BULLETIN

Týždeň 16. 09. 2020 - 22. 09. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Apple produkty - viacero zraniteľností	Vysoká	**8.8**
02.	Jenkins plugins - viacero zraniteľností	Vysoká	**8.8**
03.	Google Chrome - viacero zraniteľností	Vysoká	**8.8**
04.	Mozilla Firefox - viacero zraniteľností	Vysoká	**8.8**
05.	Advantech WebAccess Node - bezpečnostná zraniteľnosť	Vysoká	**7.8**
06.	Drupal CMS - viacero zraniteľností	Vysoká	**7.5**
07.	Adobe Media Encoder - viacero zraniteľností	Vysoká	**7.1**
08.	Philips Clinical Collaboration Platform - viacero zraniteľností	Stredná	**6.8**

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-229

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

Identifikátor

Apple produkty - viacero zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.09.2020

CVE

CVE-2020-9773, CVE-2020-9946, CVE-2020-9948, CVE-2020-9951, CVE-2020-9952, CVE-2020-9958, CVE-2020-9959, CVE-2020-9964, CVE-2020-9968, CVE-2020-9973, CVE-2020-9976, CVE-2020-9979, CVE-2020-9983, CVE-2020-9992

Zasiahnuté systémy

tvOS verzie staršie ako 14.0
iOS verzie staršie ako 14.0
iPadOS verzie staršie ako 14.0
Xcode verzie staršie ako 12.0
Safari verzie staršie ako 14.0
watchOS verzie staršie ako 7.0

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov, nenavštevovali nedôveryhodné webové stránky a neinštalovali neoverené aplikácie.
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://support.apple.com/en-us/HT211843 https://support.apple.com/en-us/HT211844 https://support.apple.com/en-us/HT211845 https://support.apple.com/en-us/HT211848 https://support.apple.com/en-us/HT211850 https://talosintelligence.com/vulnerability_reports/TALOS-2020-1124 https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2020-131/ https://exchange.xforce.ibmcloud.com/vulnerabilities/188421 https://exchange.xforce.ibmcloud.com/vulnerabilities/188418 https://exchange.xforce.ibmcloud.com/vulnerabilities/188417 https://exchange.xforce.ibmcloud.com/vulnerabilities/188409

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 nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.09.2020

CVE

CVE-2020-2252, CVE-2020-2253, CVE-2020-2254, CVE-2020-2255, CVE-2020-2256, CVE-2020-2257, CVE-2020-2258, CVE-2020-2259, CVE-2020-2260, CVE-2020-2261, CVE-2020-2262, CVE-2020-2263, CVE-2020-2264, CVE-2020-2265, CVE-2020-2266, CVE-2020-2267, CVE-2020-2268, CVE-2020-2269, CVE-2020-2270, CVE-2020-2271, CVE-2020-2272, CVE-2020-2273, CVE-2020-2274, CVE-2020-2275, CVE-2020-2276, CVE-2020-2277, CVE-2020-2278

Zasiahnuté systémy

Blue Ocean Plugin verzie staršie ako 1.23.3
computer-queue-plugin Plugin verzie staršie ako 1.6
Email Extension Plugin verzie staršie ako 2.76
Health Advisor by CloudBees Plugin verzie staršie ako 3.2.1
Mailer Plugin verzie staršie ako 1.32.1
Perfecto Plugin verzie staršie ako 1.18
Pipeline Maven Integration Plugin verzie staršie ako 3.9.3
Validating String Parameter Plugin verzie staršie ako 2.5
Android Lint Plugin verzia 2.6 a staršie
chosen-views-tabbar Plugin verzia 1.2 a staršie
ClearCase Release Plugin verzia 0.3 a staršie
Copy data to workspace Plugin verzia 1.0 a staršie
Coverage/Complexity Scatter Plot Plugin verzia 1.1.1 a staršie
Custom Job Icon Plugin verzia 0.2 a staršie
Description Column Plugin verzia 1.3 a staršie
ElasTest Plugin verzia 1.2.1 a staršie
Locked Files Report Plugin verzia 1.6 a staršie
MongoDB Plugin verzia 1.3 a staršie
Radiator View Plugin verzia 1.29 a staršie
Selection tasks Plugin verzia 1.0 a staršie
Storable Configs Plugin verzia 1.0 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.jenkins.io/security/advisory/2020-09-16/ https://exchange.xforce.ibmcloud.com/vulnerabilities/188349 https://exchange.xforce.ibmcloud.com/vulnerabilities/188367

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 zraniteľnosti by vzdialený neautentifikovaný útočník mohol prostredníctvom podvrhnutia špeciálne upraveného webového obsahu zneužiť na vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.09.2020

CVE

CVE-2020-15960, CVE-2020-15961, CVE-2020-15962, CVE-2020-15963, CVE-2020-15964, CVE-2020-15965, CVE-2020-15966

Zasiahnuté systémy

Google Chrome verzie staršie ako 85.0.4183.121

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, intergity 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/2020/09/stable-channel-update-for-desktop_21.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15962
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15964

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

Identifikátor

Mozilla Firefox - viacero zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox a Firefox ESR, ktoré opravujú viacero 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

22.09.2020

CVE

CVE-2020-15673, CVE-2020-15674, CVE-2020-15675, CVE-2020-15676, CVE-2020-15677, CVE-2020-15678

Zasiahnuté systémy

Firefox verzie staršie ako 81
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/mfsa2020-42/
https://www.mozilla.org/en-US/security/advisories/mfsa2020-43/

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

Identifikátor

Advantech WebAccess Node - bezpečnostná zraniteľnosť

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt WebAccess Node, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá na zasiahnutom systéme a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.09.2020

CVE

CVE-2020-16202

Zasiahnuté systémy

WebAccess Node verzie staršie ako 9.0.1

Následky

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

Odporúčania

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

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-261-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
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 prostredníctvom XSS útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

16.09.2020

CVE

CVE-2020-13666, CVE-2020-13667, CVE-2020-13668, CVE-2020-13669, CVE-2020-13670

Zasiahnuté systémy

Drupal verzie staršie ako 9.0.6, 8.9.6, 8.8.10, 7.73

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-2020-007
https://www.drupal.org/sa-core-2020-008
https://www.drupal.org/sa-core-2020-009
https://www.drupal.org/sa-core-2020-010
https://www.drupal.org/sa-core-2020-011
https://us-cert.cisa.gov/ncas/current-activity/2020/09/17/drupal-releases-security-updates
https://www.securityweek.com/information-disclosure-xss-vulnerabilities-patched-drupal

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

Identifikátor

Adobe Media Encoder - viacero zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Adobe Media Encoder, ktorá opravuje tri bezpečnostné zraniteľnosti.
Zraniteľnosti by lokálny neautentifikovaný útočník mohol zneužiť na získanie prístupu k citlivým údajom uloženým v pamäti zraniteľných systémov.

Dátum prvého zverejnenia varovania

15.09.2020

CVE

CVE-2020-9739, CVE-2020-9744, CVE-2020-9745

Zasiahnuté systémy

Adobe Media Encoder verzie 14.3.2 a staršie

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/media-encoder/apsb20-57.html

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Philips Clinical Collaboration Platform - viacero zraniteľností

Popis

Spoločnosť Philips vydala bezpečnostnú aktualizáciu na svoj produkt Clinical Collaboration Platform, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a tiež spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.09.2020

CVE

CVE-2020-14506, CVE-2020-14525, CVE-2020-16198, CVE-2020-16200, CVE-2020-16247

Zasiahnuté systémy

Philips Clinical Collaboration Platform verzie staršie ako 12.2.1.5

Následky

Neoprávnený prístup do systému
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.usa.philips.com/healthcare/about/customer-support/product-security
https://us-cert.cisa.gov/ics/advisories/icsma-20-261-01