BEZPEČNOSTNÝ BULLETIN

Týždeň 25. 09. 2019 - 01. 10. 2019

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:
01380/2019/SK-CERT-234

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

Identifikátor

Adobe ColdFusion zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt ColdFusion, 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

24.09.2019

CVE

CVE-2019-8072, CVE-2019-8073, CVE-2019-8074

Zasiahnuté systémy

Adobe ColdFusion 2018 verzie staršie ako Update 5
Adobe ColdFusion 2016 verzie staršie ako Update 12

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.

Zdroje

https://helpx.adobe.com/security/products/coldfusion/apsb19-47.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-coldfusion-could-allow-for-arbitrary-code-execution-apsb19-47_2019-097/
https://exchange.xforce.ibmcloud.com/vulnerabilities/167508

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

Identifikátor

LibreOffice zraniteľnosti

Popis

Vývojári kancelárskeho balíka LibreOffice vydali bezpečnostnú aktualizáciu na svojho produktu, ktorá opravuje kritickú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov v komponente LibreLogo 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

06.09.2019

CVE

CVE-2019-9855

Zasiahnuté systémy

LibreOffice verzie staršie ako 6.2.7 a 6.3.1

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.libreoffice.org/about-us/security/advisories/cve-2019-9855/
https://www.cisecurity.org/advisory/a-vulnerability-in-libreoffice-could-allow-for-arbitrary-command-execution_2019-098/

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

Identifikátor

Zraniteľnosti Apple produktov

Popis

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

Dátum prvého zverejnenia varovania

26.09.2019

CVE

CVE-2019-3855, CVE-2019-8641, CVE-2019-8654, CVE-2019-8704, CVE-2019-8721, CVE-2019-8722, CVE-2019-8723, CVE-2019-8724, CVE-2019-8725, CVE-2019-8738, CVE-2019-8739, CVE-2019-8775

Zasiahnuté systémy

Xcode verzie staršie ako 11.0
tvOS verzie staršie ako 13
Safari verzie staršie ako 13.0.1
iOS verzie staršie ako 13.1
iPadOS verzie staršie ako 13.1
watchOS verzie staršie ako 5.3.2
macOS Mojave 10.14.6, Security Update 2019-005 High Sierra, Security Update 2019-005 Sierra

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://support.apple.com/en-us/HT210588
https://support.apple.com/en-us/HT210589
https://support.apple.com/en-us/HT210590
https://support.apple.com/en-us/HT210603
https://support.apple.com/en-us/HT210604
https://support.apple.com/en-us/HT210605
https://support.apple.com/en-us/HT210609
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-products-could-allow-for-arbitrary-code-execution_2019-099/

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

Identifikátor

Foxit Reader zraniteľnosti

Popis

Spoločnosť Foxit Software vydala bezpečnostnú aktualizáciu na svoj produkt Foxit Reader, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti v komponente V8 umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia upravených PDF súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.09.2019

CVE

CVE-2019-13123, CVE-2019-13124, CVE-2019-5031

Zasiahnuté systémy

Foxit Reader verzie staršie ako 9.7

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

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

Identifikátor

PHP viacero zraniteľností

Popis

Vývojári programovacieho jazyka PHP vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť vo funkcii mb_eregi() umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.09.2019

CVE

-

Zasiahnuté systémy

PHP verzie staršie ako 7.3.10
PHP verzie staršie ako 7.2.23
PHP verzie staršie ako 7.1.30

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.

Zdroje

https://www.php.net/ChangeLog-7.php#7.3.10
https://www.php.net/ChangeLog-7.php#7.2.23
https://www.cisecurity.org/advisory/a-vulnerability-in-php-could-allow-for-arbitrary-code-execution_2019-101/

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

Identifikátor

Zraniteľnosti produktov Cisco IOS a NX-OS

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie svoje produkty IOS a NX-OS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

25.09.2019

CVE

CVE-2019-12646, CVE-2019-12647, CVE-2019-12648, CVE-2019-12649, CVE-2019-12650, CVE-2019-12651, CVE-2019-12652, CVE-2019-12653, CVE-2019-12654, CVE-2019-12655, CVE-2019-12656, CVE-2019-12657, CVE-2019-12658, CVE-2019-12659, CVE-2019-12660, CVE-2019-12661, CVE-2019-12662, CVE-2019-12663, CVE-2019-12664, CVE-2019-12665, CVE-2019-12666, CVE-2019-12667, CVE-2019-12668, CVE-2019-12669, CVE-2019-12670, CVE-2019-12671, CVE-2019-12672, CVE-2019-12709, CVE-2019-12717

Zasiahnuté systémy

Cisco IOS XR
Cisco IOS XE
Cisco NX-OS

Následky

Zneprístupnenie služby
Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-awr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-ctspac-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-http-client
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-dt
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-httpserv-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-iosxe-codeexec
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-iosxe-ctbypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-iox-gs
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-isdn-data-leak
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-nxos-vman-cmd-inj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-sbxss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-tsec
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-vman
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-vman-cmd-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-xr-asr9k-privesc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-xss
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-identd-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-iosxe-digsig-bypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-utd
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-ftp
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-iox
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-iosxe-fsdos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-rawtcp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-sip-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-webui-cmd-injection
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-ios-gos-auth
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-cat4000-tcp-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-sip-alg

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

Identifikátor

eBrigade zraniteľnosti

Popis

Vývojári aplikácie eBrigade vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injekcie získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

26.09.2019

CVE

CVE-2019-16743, CVE-2019-16744, CVE-2019-16745

Zasiahnuté systémy

eBrigade verzie staršie ako 5.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

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://seclists.org/fulldisclosure/2019/Sep/34