BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 04. 2018 – 24. 04. 2018

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:
02049/2018/TS/OKB-040

BEZPEČNOSTNÝ BULLETIN

Týždeň 18. 04. 2018 – 24. 04. 2018

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

Identifikátor

Multiple Vulnerabilities in Foxit PDF Reader

Popis

Spoločnosť Foxit vydala bezpečnostné aktualizácie na svoje produkty Foxit PDF Reader a Foxit PhantomPDF, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálneho PDF súboru mohol zneužiť na vykonanie škodlivého kódu.
Ostatné zraniteľnosti spočívajúce v nesprávnom parsovaní súborov a nedostatočnom overovaní používateľských vstupov by vzdialený neautentifikovaný útočník mohol zneužiť na neoprávnený prístup k citlivými údajom a potenciálne vykonanie škodlivého kódu.

Dátum prvého zverejnenia varovania

19.04.2018

CVE

CVE-2018-3842, CVE-2018-3843, CVE-2018-3850, CVE-2018-3853, CVE-2018-9935, CVE-2018-9936, CVE-2018-9937, CVE-2018-9938, CVE-2018-9939, CVE-2018-9940, CVE-2018-9941, CVE-2018-9942, CVE-2018-9943, CVE-2018-9944, CVE-2018-9945, CVE-2018-9946, CVE-2018-9947, CVE-2018-9948, CVE-2018-9949, CVE-2018-9950, CVE-2018-9951, CVE-2018-9952, CVE-2018-9953, CVE-2018-9954, CVE-2018-9955, CVE-2018-9956, CVE-2018-9957, CVE-2018-9958, CVE-2018-9959, CVE-2018-9960, CVE-2018-9961, CVE-2018-9962, CVE-2018-9963, CVE-2018-9964, CVE-2018-9965, CVE-2018-9966, CVE-2018-9967, CVE-2018-9968, CVE-2018-9969, CVE-2018-9970, CVE-2018-9971, CVE-2018-9972, CVE-2018-9973, CVE-2018-9974, CVE-2018-9975, CVE-2018-1173, CVE-2018-1174, CVE-2018-1175, CVE-2018-1176, CVE-2018-1177, CVE-2018-1178, CVE-2018-1179, CVE-2018-1180, CVE-2017-14458, CVE-2017-17557

Zasiahnuté systémy

Foxit PDF Reader 8.3.2.25013, 9.0.1.1049
Foxit PhantomPDF 9.0.1.1049

Následky

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

Odporúčania

Používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.foxitsoftware.com/support/security-bulletins.php#content-2018
https://securitytracker.com/id/1040733
https://blog.talosintelligence.com/2018/04/multiple-vulns-foxit-pdf-reader.html

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

Identifikátor

Microsoft Internet Explorer Remote Code Execution Vulnerability

Popis

Produkt Microsoft Internet Explorer obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník prostredníctvom podvrhnutia špeciálne vytvorených Office dokumentov obsahujúcich odkaz na webovú stránku mohol zneužiť na vykonanie škodlivého kódu.
Uvedená zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

23.04.2018

CVE

-

Zasiahnuté systémy

Microsoft Internet Explorer 10
Microsoft Internet Explorer 11

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a prílohy z neznámych zdrojov. Tiež odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.

Zdroje

https://securitytracker.com/id/1040735
https://exchange.xforce.ibmcloud.com/vulnerabilities/142119
https://www.bleepingcomputer.com/news/security/internet-explorer-zero-day-exploited-in-the-wild-by-apt-group/
https://isc.sans.edu/diary/23581

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

Identifikátor

Squid Denial of Service Vulnerability

Popis

Spoločnosť Squid Software Foundation vydala bezpečnostnú aktualizáciu, ktorá opravuje zraniteľnosť v produkte Squid.
Bezpečnostná zraniteľnosť spočíva v nesprávnom spracovávaní ESI odpovedí a vzdialený neautentifikovaný útočník by ju prostredníctvom podvrhnutia ESI odpovedí mohol zneužiť na zneprístupnenie služby. Zraniteľnosť je možné zneužiť len na Squid pracujúcich ako reverzné proxy.

Dátum prvého zverejnenia varovania

18.04.2018

CVE

CVE-2018-1172

Zasiahnuté systémy

Squid verzie 3.1.12.2 až 3.1.23
Squid verzie 3.2.0.8 až 3.2.14
Squid verzie 3.3 až 4.0.12

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://www.squid-cache.org/Advisories/SQUID-2018_3.txt
https://www.zerodayinitiative.com/advisories/ZDI-18-309/

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

Identifikátor

phpMyAdmin CSRF Vulnerability

Popis

phpMyAdmin obsahuje bezpečnostnú zraniteľnosť, ktorú by vzdialený neautentifikovaný útočník prostredníctvom CSRF (Cross-Site Request Forgery) útoku mohol zneužiť na vykonanie SQL dopytov a modifikáciu údajov v databáze.
Zraniteľnosti sa nachádzajú v:

js/db_operations.js
js/tbl_operations.js
libraries/classes/Operations.php
sql.php

Dátum prvého zverejnenia varovania

17.04.2018 (posledná aktualizácia 19.04.2018)

CVE

CVE-2018-10188

Zasiahnuté systémy

phpMyAdmin verzie 4.8.0

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.phpmyadmin.net/security/PMASA-2018-2/
https://securityonline.info/phpmyadmin-4-8-0-1-was-released-to-fix-csrf-cve-2018-10188-vulnerability/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.5**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Fineract Multiple Vulnerabilities

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Fineract, ktorý obsahuje viacero zraniteľností umožňujúcich realizáciu útoku typu SQL injekcia.
Bezpečnostnú zraniteľnosť by vzdialený autentifikovaný útočník prostredníctvom špeciálnych SQL dopytov mohol zneužiť na neoprávnený prístup a modifikáciu údajov v databáze.

Dátum prvého zverejnenia varovania

19.04.2018

CVE

CVE-2018-1289, CVE-2018-1290, CVE-2018-1291, CVE-2018-1292

Zasiahnuté systémy

Apache Fineract 0.4.0-incubating
Apache Fineract 0.5.0-incubating
Apache Fineract 0.6.0-incubating
Apache Fineract 1.0.0

Následky

Neoprávnená zmena v systéme, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

http://seclists.org/oss-sec/2018/q2/57
https://exchange.xforce.ibmcloud.com/vulnerabilities/142081
https://exchange.xforce.ibmcloud.com/vulnerabilities/142080
https://exchange.xforce.ibmcloud.com/vulnerabilities/142079
https://exchange.xforce.ibmcloud.com/vulnerabilities/142078

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 6.3**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

VMware Horizon DaaS Security Bypass Vulnerability

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt VMware Horizon DaaS, ktorá opravuje bezpečnostnú zraniteľnosť spočívajúcu v nesprávnej implementácii mechanizmov autentifikácie.
Bezpečnostnú zraniteľnosť by vzdialený útočník s platným kontom na Horizon DaaS mohol zneužiť na obídenie dvojfaktorovej autentifikácie a neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

19.04.2018

CVE

CVE-2018-6960

Zasiahnuté systémy

VMware Horizon DaaS 7.0

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých produktov.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2018-0010.html
https://tools.cisco.com/security/center/viewAlert.x?alertId=57547
https://exchange.xforce.ibmcloud.com/vulnerabilities/142089

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre: 5.4**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

CKEditor Cross-Site Scripting

Popis

Spoločnosť CKSource vydala bezpečnostnú aktualizáciu na svoju JavaScript-ovú knižnicu CKEditor, ktorá opravuje bezpečnostnú zraniteľnosť v plugine Enhanced Image (image2). Uvedená zraniteľnosť spočíva v nesprávnom overovaní používateľských vstupov a vzdialený autentifikovaný útočník by ju mohol zneužiť na vykonanie XSS (Cross-Site Scripting) útoku a neoprávnený prístup k autentifikačným údajom na báze cookies v systémoch na správu obsahu využívajúcich túto knižnicu.
V súvislosti s touto zraniteľnosťou bola vydaná aj bezpečnostná aktualizácia systému pre správu obsahu Drupal, ktorý knižnicu CKEditor aktívne využíva.

Dátum prvého zverejnenia varovania

17.04.2018

CVE

CVE-2018-9861

Zasiahnuté systémy

CKEditor verzie 4.5.11 až 4.9.1

Následky

Neoprávnený prístup k citlivými údajom

Odporúčania

Odporúčame overiť, či Vaše webové stránky nevyužívajú knižnicu CKEditor v zraniteľných verziách. V prípade, že áno, vykonajte bezodkladne aktualizáciu danej knižnice na verziu 4.9.2.

Zdroje

https://ckeditor.com/blog/CKEditor-4.9.2-with-a-security-patch-released/
https://www.drupal.org/sa-core-2018-003
https://exchange.xforce.ibmcloud.com/vulnerabilities/142056

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:
02049/2018/TS/OKB-021