BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 04. 2019 - 30. 04. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Zraniteľnosti produktov Foxit	Vysoká	**7.8**
03.	Node.js jwt-simple modul zraniteľnosť	Vysoká	**7.5**
04.	BIND zraniteľnosť	Vysoká	**7.5**
05.	Apache Solr zraniteľnosť	Vysoká	**7.5**
06.	jQuery zraniteľnosť	Stredná	**6.1**

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/TS/OKB-121

BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 04. 2019 - 30. 04. 2019

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 bezpečnostných zraniteľností.
Najzávažnejšie z týchto zraniteľností 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

23.04.2019

CVE

CVE-2019-5805, CVE-2019-5806, CVE-2019-5807, CVE-2019-5808, CVE-2019-5809, CVE-2019-5810, CVE-2019-5811, CVE-2019-5812, CVE-2019-5813, CVE-2019-5814, CVE-2019-5815, CVE-2019-5816, CVE-2019-5817, CVE-2019-5818, CVE-2019-5819, CVE-2019-5820, CVE-2019-5821, CVE-2019-5822, CVE-2019-5823

Zasiahnuté systémy

Google Chrome verzie staršie ako 74.0.3729.108

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://chromereleases.googleblog.com/2019/04/stable-channel-update-for-desktop_23.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/160081
https://exchange.xforce.ibmcloud.com/vulnerabilities/160082
https://exchange.xforce.ibmcloud.com/vulnerabilities/160083
https://exchange.xforce.ibmcloud.com/vulnerabilities/160084
https://exchange.xforce.ibmcloud.com/vulnerabilities/160085
https://exchange.xforce.ibmcloud.com/vulnerabilities/160086
https://exchange.xforce.ibmcloud.com/vulnerabilities/160087
https://exchange.xforce.ibmcloud.com/vulnerabilities/160088
https://exchange.xforce.ibmcloud.com/vulnerabilities/160089
https://exchange.xforce.ibmcloud.com/vulnerabilities/160090
https://exchange.xforce.ibmcloud.com/vulnerabilities/160091
https://exchange.xforce.ibmcloud.com/vulnerabilities/160092
https://exchange.xforce.ibmcloud.com/vulnerabilities/160093
https://exchange.xforce.ibmcloud.com/vulnerabilities/160094

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/TS/OKB-121

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

Identifikátor

Zraniteľnosti produktov Foxit

Popis

Spoločnosť Foxit Software vydala bezpečnostné aktualizácie na svoje produkty Foxit Reader a PhantomPDF, ktoré opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a 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

16.04.2019

CVE

CVE-2019-6755, CVE-2019-6756, CVE-2019-6757, CVE-2019-6758, CVE-2019-6759, CVE-2019-6760, CVE-2019-6761, CVE-2019-6762, CVE-2019-6763, CVE-2019-6764, CVE-2019-6765, CVE-2019-6766, CVE-2019-6767, CVE-2019-6768, CVE-2019-6769, CVE-2019-6770, CVE-2019-6771, CVE-2019-6772, CVE-2019-6773

Zasiahnuté systémy

Foxit Reader verzie staršie ako 9.5
Foxit PhantomPDF verzie staršie ako 9.5 a 8.3.10

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.foxitsoftware.com/support/security-bulletins.php
https://www.zerodayinitiative.com/advisories/ZDI-19-443/
https://www.zerodayinitiative.com/advisories/ZDI-19-438/
https://www.zerodayinitiative.com/advisories/ZDI-19-435/
https://www.zerodayinitiative.com/advisories/ZDI-19-426/

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

Identifikátor

Node.js jwt-simple modul zraniteľnosť

Popis

Vývojári Node.js modulu jwt-simple vydali aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

24.04.2019

CVE

Zasiahnuté systémy

Node.js jwt-simple modul verzie staršie ako 0.5.3

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.npmjs.com/advisories/831
https://exchange.xforce.ibmcloud.com/vulnerabilities/160132

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

Identifikátor

BIND zraniteľnosť

Popis

Vývojári DNS servera BIND vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

24.04.2019

CVE

CVE-2018-5743, CVE-2019-6467, CVE-2019-6468

Zasiahnuté systémy

BIND verzie staršie ako 9.11.6-P1, 9.12.4-P1 a 9.14.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.isc.org/docs/cve-2018-5743
https://kb.isc.org/docs/cve-2019-6468
https://kb.isc.org/docs/cve-2019-6467

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

Identifikátor

Apache Solr zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache Solr, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

24.04.2019

CVE

CVE-2018-11802

Zasiahnuté systémy

Apache Solr verzie staršie ako 7.7 a 6.6.6

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://mail-archives.apache.org/mod_mbox/lucene-dev/201904.mbox/%3CCAHPRk5HKN=LmhXz4xoKE6LCp6GbcEQQob9JWA9pV8kqQfuJVkw@mail.gmail.com%3E

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

jQuery zraniteľnosť

Popis

Vývojári JavaScriptovej knižnice jQuery vydali aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom Cross-Site Scripting (XSS) útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

24.04.2019

CVE

CVE-2019-11358

Zasiahnuté systémy

jQuery verzie staršie ako 3.4.0

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://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
https://tools.cisco.com/security/center/viewAlert.x?alertId=60052