BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 05. 2019 - 14. 05. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Kaspersky Lab Antivirus Engine zraniteľnosť	Vysoká	**8.8**
02.	LibreOffice zraniteľnosť	Vysoká	**8.8**
03.	SQLite zraniteľnosť	Vysoká	**8.1**
04.	Ghostscript zraniteľnosť	Vysoká	**7.6**
05.	CyberArk Enterprise Password Vault zraniteľnosť	Vysoká	**7.5**
06.	Spring moduly viacero zraniteľností	Vysoká	**7.3**
07.	PostgreSQL viacero bezpečnostných zraniteľností	Vysoká	**7.0**
08.	OneShield Policy (Dragon Core) framework zraniteľnosť	Stredná	**6.1**
09.	Symantec AV Engine For Mac zraniteľnosť	Stredná	**5.1**

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-139

BEZPEČNOSTNÝ BULLETIN

Týždeň 08. 05. 2019 - 14. 05. 2019

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

Identifikátor

Kaspersky Lab Antivirus Engine zraniteľnosť

Popis

Spoločnosť Kaspersky vydala bezpečnostnú aktualizáciu na svoj produkt Kaspersky Lab Antivirus Engine, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.05.2019

CVE

CVE-2019-8285

Zasiahnuté systémy

Kaspersky Lab Antivirus Engine verzie staršie ako 04.apr.2019

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://nvd.nist.gov/vuln/detail/CVE-2019-8285
https://support.kaspersky.com/vulnerability.aspx?el=12430#080519

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

Identifikátor

LibreOffice zraniteľnosť

Popis

Vývojári kancelárskeho balíka LibreOffice vydali aktualizácie na svoj produkt, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním hypertextových odkazov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

08.05.2019

CVE

CVE-2019-9847

Zasiahnuté systémy

LibreOffice pre Windows a macOS verzie staršie ako 6.1.6 a 6.2.3

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.libreoffice.org/about-us/security/advisories/cve-2019-9847/
https://tools.cisco.com/security/center/viewAlert.x?alertId=60165

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SQLite zraniteľnosť

Popis

Vývojári databázového systému SQLite vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.05.2019

CVE

CVE-2019-5018

Zasiahnuté systémy

SQLite verzie staršie ako SQLite 3.28.0

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.talosintelligence.com/vulnerability_reports/TALOS-2019-0777
https://blog.talosintelligence.com/2019/05/vulnerability-spotlight-remote-code.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Ghostscript zraniteľnosť

Popis

Spoločnosť Artifex vydala aktualizáciu na svoj produkt Ghostscript, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špecialne vytvoreného PostScript súboru získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

09.05.2019

CVE

CVE-2019-3839

Zasiahnuté systémy

Ghostscript verzie staršie ako 9.27

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://bugs.ghostscript.com/show_bug.cgi?id=700317
https://tools.cisco.com/security/center/viewAlert.x?alertId=60111

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

Identifikátor

CyberArk Enterprise Password Vault zraniteľnosť

Popis

Spoločnosť CyberArk vydala bezpečnostnú aktualizáciu na svoj produkt CyberArk Enterprise Password Vault, ktorá opravuje bezpečnostnú zraniteľnosť v komponente SAML.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XXE útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

19.02.2019

CVE

CVE-2019-7442

Zasiahnuté systémy

CyberArk Enterprise Password Vault verzie staršie ako 10.7

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://www.octority.com/2019/05/07/cyberark-enterprise-password-vault-xml-external-entity-xxe-injection/
https://nvd.nist.gov/vuln/detail/CVE-2019-7442

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Spring moduly viacero zraniteľností

Popis

Vývojári Spring vydali aktualizácie na moduly spring-cloud-config a spring-data-jpa, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nesprávnym spracovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

16.04.2019

CVE

CVE-2019-3797, CVE-2019-3799

Zasiahnuté systémy

spring-cloud-config verzie staršie ako 2.1.2, 2.0.4 a 1.4.6
spring-data-jpa verzie staršie ako 2.1.6, 2.0.14 a 1.11.20

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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://pivotal.io/security/cve-2019-3799
https://pivotal.io/security/cve-2019-3797
https://tools.cisco.com/security/center/viewAlert.x?alertId=60112
https://tools.cisco.com/security/center/viewAlert.x?alertId=60113

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.0
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

PostgreSQL viacero bezpečnostných zraniteľností

Popis

Vývojári databázového systému PostgreSQL vydali aktualizácie na svoj produkt, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.05.2019

CVE

CVE-2019-10127, CVE-2019-10128

Zasiahnuté systémy

PostgreSQL verzie staršie ako 11.3, 10.8, 9.6.13, 9.5.17 a 9.4.22

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.postgresql.org/about/news/1939/
https://tools.cisco.com/security/center/viewAlert.x?alertId=60166
https://tools.cisco.com/security/center/viewAlert.x?alertId=60167

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

Identifikátor

OneShield Policy (Dragon Core) framework zraniteľnosť

Popis

Spoločnosť OneShield vydala bezpečnostnú aktualizáciu na svoj produkt Policy (Dragon) framework, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

01.05.2019

CVE

CVE-2019-11643

Zasiahnuté systémy

OneShield Policy (Dragon Core) framework verzie staršie ako 5.1.10

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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/May/2
https://nvd.nist.gov/vuln/detail/CVE-2019-11643

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Symantec AV Engine For Mac zraniteľnosť

Popis

Spoločnosť Symantec vydala bezpečnostnú aktualizáciu na svoj produkt AV Engine pre Mac, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

01.05.2019

CVE

CVE-2019-9698

Zasiahnuté systémy

Symantec AV Engine For Mac verzie staršie ako 13.0.9r17

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.symantec.com/en_US/article.SYMSA1481.html