BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 11. 2019 - 03. 12. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox zraniteľnosti	Vysoká	**8.8**
02.	MOTEX LanScope Cat and An zraniteľnosť	Vysoká	**7.8**
03.	Kaspersky produkty viacero zraniteľností	Vysoká	**7.5**
04.	Forma LMS viacero zraniteľností	Vysoká	**7.4**
05.	Artifex Ghostscript zraniteľnosť	Vysoká	**7.3**

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-279

BEZPEČNOSTNÝ BULLETIN

Týždeň 27. 11. 2019 - 03. 12. 2019

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

Identifikátor

Mozilla Firefox zraniteľnosti

Popis

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

03.12.2019

CVE

CVE-2019-11745, CVE-2019-11756, CVE-2019-13722, CVE-2019-17005, CVE-2019-17008, CVE-2019-17009, CVE-2019-17010, CVE-2019-17011, CVE-2019-17012, CVE-2019-17013, CVE-2019-17014

Zasiahnuté systémy

Firefox verzie staršie ako 71
Firefox ESR verzie staršie ako 68.3

Následky

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

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.mozilla.org/en-US/security/advisories/mfsa2019-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-37/

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

Identifikátor

MOTEX LanScope Cat and An zraniteľnosť

Popis

Spoločnosť MOTEX vydala bezpečnostnú aktualizáciu na svoje produkty LanScope Cat a LanScope An, ktorá opravuje bezpečnostnú zraniteľnosť.
Bližšie nešpecifikovaná bezpečnostná zraniteľnosť umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

02.12.2019

CVE

CVE-2019-6026

Zasiahnuté systémy

LanScope Cat verzie staršie ako 9.2.1.0 a 9.2.2.0
LanScope An verzie staršie ako 2.7.7.0 (LanScope An 2 series) a 3.0.8.1 (LanScope An 3 series)

Následky

Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://jvn.jp/en/jp/JVN49068796/
https://www.motex.co.jp/news/notice/2019/release191202/

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

Identifikátor

Kaspersky produkty viacero zraniteľností

Popis

Spoločnosť Kaspersky vydala bezpečnostné aktualizácie na portfólio svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.11.2019

CVE

CVE-2019-15684, CVE-2019-15685, CVE-2019-15686, CVE-2019-15687, CVE-2019-15688, CVE-2019-15689

Zasiahnuté systémy

Kaspersky Password Manager for Windows verzie staršie ako 9.2.
Kaspersky Secure Connection verzie staršie ako 4.0 (2020) patch E.
Kaspersky Internet Security verzie staršie ako 2020 patch E.
Kaspersky Total Security verzie staršie ako 2020 patch E.
Kaspersky Security Cloud verzie staršie ako 2020 patch E.
Kaspersky Anti-Virus verzie staršie ako 2019 Patch I, Patch J
Kaspersky Free Anti-Virus verzie staršie ako 2019 Patch I, Patch J
Kaspersky Small Office Security verzie staršie ako 6 Patch I, Patch J
Kaspersky Protection extension for Google Chrome verzie staršie ako 20.0.543.1418 as a part of 2019 Patch I
Kaspersky Anti-Virus verzie staršie ako 2020 Patch E, Patch F
Kaspersky Internet Security verzie staršie ako 2020 Patch E, Patch F
Kaspersky Total Security verzie staršie ako 2020 Patch E, Patch F
Kaspersky Free Anti-Virus verzie staršie ako 2020 Patch E, Patch F
Kaspersky Small Office Security verzie staršie ako 7 Patch E, Patch F
Kaspersky Protection extension for Google Chrome verzie staršie ako 30.112.62.0 as a part of 2020 Patch E

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Eskalácia privilégií

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://support.kaspersky.com/general/vulnerability.aspx?el=12430#251119_1 https://exchange.xforce.ibmcloud.com/vulnerabilities/172202

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Forma LMS viacero zraniteľností

Popis

Vývojári Forma LMS vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi prostredníctvom SQL injection útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.12.2019

CVE

CVE-2019-5109, CVE-2019-5110, CVE-2019-5111, CVE-2019-5112

Zasiahnuté systémy

Forma LMS 2.2.1

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://talosintelligence.com/vulnerability_reports/TALOS-2019-0904
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0902
https://talosintelligence.com/vulnerability_reports/TALOS-2019-0903

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

Identifikátor

Artifex Ghostscript zraniteľnosť

Popis

Spoločnosť Artifex vydala bezpečnostnú aktualizáciu na svoj produkt Ghostscript, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného PostScript súboru získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

27.11.2019

CVE

CVE-2019-14812

Zasiahnuté systémy

Artifex Ghostscript verzie staršie ako 9.50

Následky

Neoprávnený prístup do 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.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2019-14812
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14812