BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 09. 2019 - 10. 09. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox zraniteľnosti	Vysoká	**8.8**
02.	Samba zraniteľnosť	Vysoká	**8.7**
03.	EZAutomation EZ Touch Editor zraniteľnosť	Vysoká	**7.8**
04.	EZAutomation EZ PLC Editor zraniteľnosť	Vysoká	**7.8**
05.	Red Lion Controls Crimson zraniteľnosti	Vysoká	**7.8**
06.	Becton Dickinson Pyxis zraniteľnosť	Vysoká	**7.6**
07.	WordPress bezpečnostné zraniteľnosti	Vysoká	**7.5**

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-219

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 bezpečnostné zraniteľnosti.
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

03.09.2019

CVE

CVE-2019-11734, CVE-2019-11735, CVE-2019-11736, CVE-2019-11737, CVE-2019-11738, CVE-2019-11740, CVE-2019-11741, CVE-2019-11742, CVE-2019-11743, CVE-2019-11744, CVE-2019-11746, CVE-2019-11747, CVE-2019-11748, CVE-2019-11749, CVE-2019-11750, CVE-2019-11751, CVE-2019-11752, CVE-2019-11753, CVE-2019-5849, CVE-2019-9812

Zasiahnuté systémy

Firefox verzie staršie ako 69
Firefox ESR verzie staršie ako 68.1

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti

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/mfsa2019-25/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-26/
https://www.bleepingcomputer.com/news/software/firefox-69-released-with-enhanced-tracking-protection-and-flash-disabled/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Samba zraniteľnosť

Popis

Vývojári produktu Samba vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.09.2019

CVE

CVE-2019-10197

Zasiahnuté systémy

Samba verzie staršie ako 4.9.13, 4.10.8 a 4.11.0rc3

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.samba.org/samba/security/CVE-2019-10197.html

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

Identifikátor

EZAutomation EZ Touch Editor zraniteľnosť

Popis

Spoločnosť EZAutomation vydala bezpečnostnú aktualizáciu na svoj produkt EZ Touch Editor, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného súboru spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.09.2019

CVE

CVE-2019-13518

Zasiahnuté systémy

EZAutomation EZ Touch Editor verzie staršie ako 2.2.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-246-01

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

Identifikátor

EZAutomation EZ PLC Editor zraniteľnosť

Popis

Spoločnosť EZAutomation vydala bezpečnostnú aktualizáciu na svoj produkt EZ PLC Editor, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného súboru spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.09.2019

CVE

CVE-2019-13522

Zasiahnuté systémy

EZAutomation EZ PLC Editor verzie staršie ako 1.9.0

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-246-02

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

Identifikátor

Red Lion Controls Crimson zraniteľnosti

Popis

Spoločnosť Red Lion Controls vydala bezpečnostnú aktualizáciu na svoj produkt Crimson, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.09.2019

CVE

CVE-2019-10978, CVE-2019-10984, CVE-2019-10990, CVE-2019-10996

Zasiahnuté systémy

Red Lion Controls Crimson verzie staršie ako 3.1 release 3112.00

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-248-01

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

Identifikátor

Becton Dickinson Pyxis zraniteľnosť

Popis

Spoločnosť Becton Dickinson vydala bezpečnostnú aktualizáciu na svoj produkt Pyxis ES, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi, nachádzajúcemu sa v rovnakom sieťovom segmente, eskalovať svoje privilégiá na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

05.09.2019

CVE

CVE-2019-13517

Zasiahnuté systémy

Becton Dickinson Pyxis ES verzie staršie ako 1.6.1.1
Becton Dickinson Pyxis Enterprise Server, with Windows Server verzie 4.4 až 4.12

Následky

Neoprávnený prístup do systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-246-02

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

Identifikátor

WordPress bezpečnostné zraniteľnosti

Popis

Vývojári redakčného systému WordPress vydali aktualizáciu svojho produktu, ktorá opravuje šesť bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS (Cross-Site Scripting) útokov získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

05.09.2019

CVE

-

Zasiahnuté systémy

WordPress verzie staršie ako 5.2.3

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Wordpress v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a pluginov.
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://wordpress.org/news/2019/09/wordpress-5-2-3-security-and-maintenance-release/
https://www.bleepingcomputer.com/news/security/wordpress-523-released-with-security-and-bug-fixes/
https://www.securityweek.com/wordpress-523-patches-several-xss-vulnerabilities

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-219