BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 11. 2018 - 27. 11. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Atlantis Word Processor zraniteľnosti	Vysoká	**8.8**
02.	Zraniteľnosť v Adobe Flash Player	Vysoká	**8.8**
03.	Teledyne DALSA Sherlock zraniteľnosť	Vysoká	**7.3**
04.	Modicon PLC zraniteľnosť	Stredná	**6.5**
05.	Viacero zraniteľností v Samba	Stredná	**6.5**
06.	Moodle zraniteľnosť	Stredná	**6.5**

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:
02049/2018/TS/OKB-195

BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 11. 2018 - 27. 11. 2018

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

Identifikátor

Atlantis Word Processor zraniteľnosti

Popis

Vývojári textového editora Atlantis Word Processor vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostné zraniteľnosti spôsobené nesprávnym spracovaním údajov.
Bezpečnostné zraniteľnosti umožňujú vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

20.11.2018

CVE

CVE-2018-4038, CVE-2018-4039, CVE-2018-4040

Zasiahnuté systémy

Atlantis Word Processor verzie staršie ako 3.2.10.1

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 a súbory z neznámych zdrojov.

Zdroje

https://blog.talosintelligence.com/2018/11/Atlantis-Word-Processor-RCE-vulns.html
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0713
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0711
https://www.talosintelligence.com/vulnerability_reports/TALOS-2018-0712
https://thehackernews.com/2018/11/word-processor-vulnerability.html

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

Identifikátor

Zraniteľnosť v Adobe Flash Player

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Flash Player, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nesprávnom overovaní dátových typov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.11.2018

CVE

CVE-2018-15981

Zasiahnuté systémy

Adobe Flash Player verzie staršie ako 31.0.0.153

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://helpx.adobe.com/security/products/flash-player/apsb18-44.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/153055

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

Identifikátor

Teledyne DALSA Sherlock zraniteľnosť

Popis

Spoločnosť Teledyne DALSA vydala bezpečnostnú aktualizáciu na monitorovací systém Sherlock, ktorá opravuje bližšie nešpecifikovanú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje lokálnemu autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov spôsobiť pád systému alebo vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

20.11.2018

CVE

CVE-2018-17930

Zasiahnuté systémy

Teledyne DALSA Sherlock verzie staršie ako 7.2.7.5

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-324-01

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

Identifikátor

Modicon PLC zraniteľnosť

Popis

Viacero produktov od spoločnosti Schneider Electric obsahuje bezpečnostné zraniteľnosti v komponente webového servera.
Zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a umožňujú vzdialenému neautentifikovanému útočníkovi obísť mechanizmy autentifikácie, získať neoprávnený prístup do systému a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.11.2018

CVE

CVE-2018-7811, CVE-2018-7809,CVE-2018-7810, CVE-2018-7830, CVE-2018-7831

Zasiahnuté systémy

Modicon M340, Premium, Quantum PLCs a BMXNOR0200

Následky

Neoprávnený prístup do systému
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vypnúť funkciu webového servera v zasiahnutých zariadeniach a dočasne ju zapínať iba v nevyhnutných prípadoch. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2018-327-01-Embedded-Web-Servers-Modicon.pdf

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

Identifikátor

Viacero zraniteľností v Samba

Popis

Vývojári softvéru Samba vydali aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti umožňujú vzdialenému autentifikovanému útočníkovi spôsobiť zneprístupnenie služieb na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

27.11.2018

CVE

CVE-2018-16857, CVE-2018-16853, CVE-2018-16852, CVE-2018-16851, CVE-2018-16841, CVE-2018-14629

Zasiahnuté systémy

Samba verzie staršie ako 4.9.3

Následky

Zneprístupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.samba.org/samba/security/CVE-2018-14629.html
https://www.samba.org/samba/security/CVE-2018-16841.html
https://www.samba.org/samba/security/CVE-2018-16851.html
https://www.samba.org/samba/security/CVE-2018-16852.html
https://www.samba.org/samba/security/CVE-2018-16853.html
https://www.samba.org/samba/security/CVE-2018-16857.html

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

Identifikátor

Moodle zraniteľnosť

Popis

Vývojári e-learningovej platformy Moodle vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v autentifikačnom rozhraní.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom CSRF (Cross-Site Request Forgery) útoku vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

19.11.2018

CVE

CVE-2018-16854

Zasiahnuté systémy

Moodle verzie staršie ako 3.5.3

Následky

Neoprávnená zmena v systéme

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://tools.cisco.com/security/center/viewAlert.x?alertId=59194
https://moodle.org/mod/forum/discuss.php?d=378731