BEZPEČNOSTNÝ BULLETIN

Týždeň 11. 09. 2019 - 17. 09. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Google Chrome viacero zraniteľností	Vysoká	**8.8**
02.	Adobe Flash Player zraniteľnosti	Vysoká	**8.8**
03.	Adobe Application Manager zraniteľnosť	Vysoká	**8.8**
04.	Mozilla Thunderbird zraniteľnosti	Vysoká	**8.8**
05.	McAfee Endpoint Security zraniteľnosť	Vysoká	**8.1**
06.	Modicon Quantum 140 NOE771x1 zraniteľnosť	Vysoká	**8.1**
07.	Delta Electronics TPEditor zraniteľnosti	Vysoká	**7.8**
08.	Wireshark viacero zraniteľností	Vysoká	**7.5**
09.	Siemens SIMATIC TDC CP51M1 zraniteľnosť	Vysoká	**7.5**
10.	Siemens IE-WSN-PA Link WirelessHART Gateway XSS zraniteľnosť	Vysoká	**7.5**
11.	LastPass zraniteľnosť	Vysoká	**7.4**

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-224

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 prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-13659, CVE-2019-13660, CVE-2019-13661, CVE-2019-13662, CVE-2019-13663, CVE-2019-13664, CVE-2019-13665, CVE-2019-13666, CVE-2019-13667, CVE-2019-13668, CVE-2019-13669, CVE-2019-13670, CVE-2019-13671, CVE-2019-13673, CVE-2019-13674, CVE-2019-13675, CVE-2019-13676, CVE-2019-13677, CVE-2019-13678, CVE-2019-13679, CVE-2019-13680, CVE-2019-13681, CVE-2019-13682, CVE-2019-13683, CVE-2019-5870, CVE-2019-5871, CVE-2019-5872, CVE-2019-5873, CVE-2019-5874, CVE-2019-5875, CVE-2019-5876, CVE-2019-5877, CVE-2019-5878, CVE-2019-5879, CVE-2019-5880, CVE-2019-5881

Zasiahnuté systémy

Google Chrome verzie staršie ako 77.0.3865.75

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://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop.html
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-chrome-could-allow-for-arbitrary-code-execution_2019-093/

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

Identifikátor

Adobe Flash Player zraniteľnosti

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Flash Player, ktorá opravuje bezpečnostné zraniteľnosti.
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

10.09.2019

CVE

CVE-2019-8069, CVE-2019-8070

Zasiahnuté systémy

Adobe Flash Player staršie ako 32.0.0.255

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.cisecurity.org/advisory/multiple-vulnerabilities-in-adobe-flash-player-could-allow-for-arbitrary-code-execution-apsb19-46_2019-091/
https://exchange.xforce.ibmcloud.com/vulnerabilities/166563
https://exchange.xforce.ibmcloud.com/vulnerabilities/166562

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

Identifikátor

Adobe Application Manager zraniteľnosť

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Application Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov pri načítaní knižníc a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-8076

Zasiahnuté systémy

Adobe Application Manager verzia 10.0

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 súbory z neznámych zdrojov.
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://helpx.adobe.com/security/products/application_manager/apsb19-45.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/166807

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

Identifikátor

Mozilla Thunderbird zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoj e-mailový klient Thunderbird, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov 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

06.09.2019

CVE

CVE-2019-11739, CVE-2019-11740, CVE-2019-11742, CVE-2019-11743, CVE-2019-11744, CVE-2019-11746, CVE-2019-11752

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 60.9 a 68.1

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, prílohy eznámych 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/mfsa2019-30/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-29/
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-thunderbird-could-allow-for-arbitrary-code-execution_2019-094/

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

Identifikátor

McAfee Endpoint Security zraniteľnosť

Popis

Spoločnosť McAfee vydala bezpečnostnú aktualizáciu na svoj produkt Web Gateway, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov v administrátorskej webovej konzole a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených URL získať neoprávnený prístup k citlivým údajom a vykonávať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-3638

Zasiahnuté systémy

McAfee Web Gateway verzie staršie ako 7.8.2.13 a 8.2

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://kc.mcafee.com/corporate/index?page=content&id=SB10294
https://exchange.xforce.ibmcloud.com/vulnerabilities/167026

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

Identifikátor

Modicon Quantum 140 NOE771x1 zraniteľnosť

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt Modicon Quantum 140 NOE771x1, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-6811

Zasiahnuté systémy

Modicon Quantum 140 NOE771x1 verzie staršie ako 7.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. 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-2019-253-02-Modicon-Quantum-NOE.pdf&p_Doc_Ref=SEVD-2019-253-02

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

Identifikátor

Delta Electronics TPEditor zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt TPEditor, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-13536, CVE-2019-13540, CVE-2019-13544

Zasiahnuté systémy

Delta Industrial Automation TPEditor verzie staršie ako 1.95

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-19-253-01

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

Identifikátor

Wireshark viacero zraniteľností

Popis

Vývojári nástroja na analýzu sieťovej prevádzky Wireshark vydali aktualizáciu svojho produktu, ktorá rieši viaceré bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upravených paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

11.09.2019

CVE

CVE-2019-16319

Zasiahnuté systémy

Wireshark verzie staršie ako 3.0.4 a 2.6.11

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.wireshark.org/security/wnpa-sec-2019-21
https://gbhackers.com/wireshark-3-0-4-released/amp/

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

Identifikátor

Siemens SIMATIC TDC CP51M1 zraniteľnosť

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoj produkt SIMATIC TDC CP51M1, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených UDP paketov spôsobiť zneprístupnenie služieb.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-10937

Zasiahnuté systémy

Siemens SIMATIC TDC CP51M1 verzie staršie ako 1.1.7

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Tiež odporúčame aplikovať firewallové pravidlá a blokovať UDP komunikáciu.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-250618.pdf
https://www.us-cert.gov/ics/advisories/icsa-19-253-05

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

Identifikátor

Siemens IE-WSN-PA Link WirelessHART Gateway XSS zraniteľnosť

Popis

Spoločnosť Siemens informuje o bezpečnostnej zraniteľnosti v komunikačných bránach IE/WSN-PA Link.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciu bezpečnostných mechanizmov v konfiguračnom webovom serveri a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom Cross-Site Scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.09.2019

CVE

CVE-2019-13923

Zasiahnuté systémy

IE/WSN-PA Link WirelessHART Gateway

Následky

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

Odporúčania

Spoločnosť Siemens doposiaľ nevydala aktualizáciu riešiacu uvedenú zraniteľnosť. Administrátorom konfigurujúcim zraniteľné zariadenia odporúčame, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://cert-portal.siemens.com/productcert/pdf/ssa-191683.pdf
https://www.us-cert.gov/ics/advisories/icsa-19-253-04

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

Identifikátor

LastPass zraniteľnosť

Popis

Vývojári správcu hesiel LastPass vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii do_popupregister().
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne upraveného webového obsahu získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

12.09.2019

CVE

CVE-2019-16371

Zasiahnuté systémy

LastPass (rozšírenie pre prehliadač Chrome a Opera) verzie staršie ako 4.33.0

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.lastpass.com/2019/09/lastpass-bug-reported-resolved.html/
https://www.theregister.co.uk/2019/09/16/lastpass_vulnerability/
https://nvd.nist.gov/vuln/detail/CVE-2019-16371
https://siliconangle.com/2019/09/16/lastpass-fixes-bug-allowed-malicious-websites-steal-login-credentials/

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-224