BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 07. 2019 - 16. 07. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Mozilla Firefox zraniteľnosti	Vysoká	**8.8**
02.	Jira server a Jira Data Center zraniteľnosť	Vysoká	**8.4**
03.	Siemens Tia Administrator (TIA Portal) zraniteľnosť	Vysoká	**8.0**
04.	Delta Industrial Automation CNCSoft ScreenEditor viacero zraniteľností	Vysoká	**7.8**
05.	ABB CCLAS a Ellipse zraniteľnosti	Vysoká	**7.5**
06.	MatrixSSL ASN.1 zraniteľnosť	Vysoká	**7.3**
07.	Schneider Electric Interactive Graphical SCADA System zraniteľnosť	Vysoká	**7.0**
08.	FFmpeg 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:
01380/2019/TS/OKB-185

BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 07. 2019 - 16. 07. 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, ktoré opravujú viacero zraniteľností v internetovom prehliadači Firefox.
Najzávažnejšie 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

09.07.2019

CVE

CVE-2019-11709, CVE-2019-11710, CVE-2019-11711, CVE-2019-11712, CVE-2019-11713, CVE-2019-11714, CVE-2019-11715, CVE-2019-11716, CVE-2019-11717, CVE-2019-11718, CVE-2019-11719, CVE-2019-11720, CVE-2019-11721, CVE-2019-11723, CVE-2019-11724, CVE-2019-11725, CVE-2019-11727, CVE-2019-11728, CVE-2019-11729, CVE-2019-11730, CVE-2019-9811

Zasiahnuté systémy

Mozilla Firefox verzie staršie ako 68
Mozilla Firefox ESR verzie staršie ako 60.8

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2019-21/#CVE-2019-11709
https://access.redhat.com/security/cve/cve-2019-11709
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mozilla-firefox-could-allow-for-arbitrary-code-execution_2019-071/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.4**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Jira server a Jira Data Center zraniteľnosť

Popis

Spoločnosť Jira vydala bezpečnostné aktualizácie na svoje produkty Jira server a Jira Data Center, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.07.2019

CVE

CVE-2019-11581

Zasiahnuté systémy

Jira Server a Jira Data Center verzie staršie ako 7.6.14
Jira Server a Jira Data Center verzie staršie ako 7.13.5
Jira Server a Jira Data Center verzie staršie ako 8.0.3
Jira Server a Jira Data Center verzie staršie ako 8.1.2
Jira Server a Jira Data Center verzie staršie ako 8.2.3
Jira Service Desk verzie staršie ako 4.2.3

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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/a-vulnerability-in-jira-server-could-allow-for-server-side-template-injection_2019-072/
https://confluence.atlassian.com/jira/jira-security-advisory-2019-07-10-973486595.html
https://www.tenable.com/blog/cve-2019-11581-critical-template-injection-vulnerability-in-atlassian-jira-server-and-data
https://www.bleepingcomputer.com/news/security/jira-server-and-data-center-update-patches-critical-vulnerability/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Siemens Tia Administrator (TIA Portal) zraniteľnosť

Popis

Spoločnosť Siemens vydala bezpečnostnú aktualizáciu na svoju webovú aplikáciu Tia Administrator (TIA Portal), ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených packetov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Proof-of-concept (PoC) kód je verejne dostupný.

Dátum prvého zverejnenia varovania

09.07.2019

CVE

CVE-2019-10915

Zasiahnuté systémy

Siemens TIA Administrator verzie staršie ako 1.0 SP1 Update 1
Siemens TIA Portal verzie staršie ako 15 Update 5

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a obmedziť prístup k portu 8888/tcp na localhost.
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.tenable.com/security/research/tra-2019-33
https://www.us-cert.gov/ics/advisories/icsa-19-192-03
https://www.securityfocus.com/bid/109124/info
https://medium.com/tenable-techblog/nuclear-meltdown-with-critical-ics-vulnerabilities-8af3a1a13e6a
https://cert-portal.siemens.com/productcert/pdf/ssa-721298.pdf

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

Identifikátor

Delta Industrial Automation CNCSoft ScreenEditor viacero zraniteľností

Popis

Spoločnosť Delta vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft ScreenEditor, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.07.2019

CVE

CVE-2019-10982, CVE-2019-10992

Zasiahnuté systémy

Delta Industrial Automation CNCSoft ScreenEditor verzie staršie ako 1.00.94.

Následky

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

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-192-01

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

Identifikátor

ABB CCLAS a Ellipse zraniteľnosti

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na svoje informačné systémy CCLAS a Ellipse, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom špeciálne vytvorenej URL adresy získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

15.07.2019

CVE

Zasiahnuté systémy

CCLAS verzie staršie ako 6.6.0.4 alebo 6.7
Ellipse verzie staršie ako 8.5.28
Ellipse verzie staršie ako 8.6.25
Ellipse verzie staršie ako 8.7.23
Ellipse verzie staršie ako 8.8.19
Ellipse verzie staršie ako 8.9.19
Ellipse verzie staršie ako 9.0.7

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=9AKK107492A6224&LanguageCode=en&DocumentPartId=&Action=Launch

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

Identifikátor

MatrixSSL ASN.1 zraniteľnosť

Popis

Vývojári kryptografického protokolu MatrixSSL vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného certifikátu vykonať škodlivý kód alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.07.2019

CVE

CVE-2019-13470

Zasiahnuté systémy

MatrixSSL verzie staršie ako 4.2.1

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby

Odporúčania

Ak váš softvér alebo zariadenie používa SSL, preverte u svojho dodávateľa, či neobsahuje knižnicu MatrixSSL. V prípade, že využívate MatrixSSL, odporúčame vykonať aktualizáciu zasiahnutých systémov. Taktiež odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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://tools.cisco.com/security/center/viewAlert.x?alertId=60454
https://github.com/matrixssl/matrixssl/blob/4-2-1-open/doc/CHANGES_v4.x.md#changes-between-420-and-421-june-2019

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

Identifikátor

Schneider Electric Interactive Graphical SCADA System zraniteľnosť

Popis

Spoločnosť Schneider vydala bezpečnostnú aktualizáciu na svoj interaktívny grafický SCADA systém, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.07.2019

CVE

CVE-2019-6827

Zasiahnuté systémy

Schneider Electric Interactive Graphical SCADA System verzie staršie ako 13.0.0.19140
Schneider Electric Interactive Graphical SCADA System verzie staršie ako 14.0.0.19120

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.us-cert.gov/ics/advisories/icsa-19-192-06

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

Identifikátor

FFmpeg zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v software na úpravu videa a zvuku FFmpeg.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.07.2019

CVE

CVE-2019-13390

Zasiahnuté systémy

FFmpeg verzia 4.1(.3)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Taktiež odporúčame aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
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=60450
https://trac.ffmpeg.org/ticket/7979