BEZPEČNOSTNÝ BULLETIN

Týždeň 24. 07. 2019 - 30. 07. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Fortinet FortiClient for Windows zraniteľnosť	Vysoká	**8.8**
02.	GNU Project patch zraniteľnosť	Vysoká	**8.8**
03.	Exim "sort" zraniteľnosť	Vysoká	**8.1**
04.	Mitsubishi Electric FR Configurator2 zraniteľnosti	Vysoká	**7.1**
05.	eClass platform zraniteľnosti	Stredná	**6.5**
06.	Poppler zraniteľnosť	Stredná	**6.5**
07.	National Renewable Energy Laboratory (NREL) EnergyPlus zraniteľnosť	Stredná	**6.1**

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-194

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

Identifikátor

Fortinet FortiClient for Windows zraniteľnosť

Popis

Spoločnosť Fortinet vydala bezpečnostnú aktualizáciu na svoj anti-vírus FortiClient for Windows, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného DLL súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.07.2019

CVE

CVE-2019-6692

Zasiahnuté systémy

Fortinet FortiClient for Windows verzie staršie ako 6.2.1

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
Do vydania aktualizácií administrátorom odporúčame zabezpečiť systém podľa návodu zverejnenom na: https://fortiguard.com/psirt/FG-IR-19-148
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://fortiguard.com/psirt/FG-IR-19-148
https://exchange.xforce.ibmcloud.com/vulnerabilities/164293

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

Identifikátor

GNU Project patch zraniteľnosť

Popis

Vývojári operačného systému GNU Project vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť knižnice GNU patch.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.07.2019

CVE

CVE-2019-13638

Zasiahnuté systémy

GNU Project patch

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame limitovať prístup k administratívnemu rozhraniu 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=60509

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

Identifikátor

Exim "sort" zraniteľnosť

Popis

Vývojári emailového systému Exim vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii ${sort}.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.07.2019

CVE

CVE-2019-13917

Zasiahnuté systémy

Exim verzie staršie ako 4.92.1

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade, že aktualizácia nie je možná, odporúčame Vám vyhnúť sa používaniu funkcie ${sort} vo Vašej konfigurácii.
Taktiež odporúčame limitovať prístup k administratívnemu rozhraniu 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://www.exim.org/static/doc/security/CVE-2019-13917.txt
https://tools.cisco.com/security/center/viewAlert.x?alertId=60504

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric FR Configurator2 zraniteľnosti

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na svoj produkt FR Configurator2, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru získať neoprávnený prístup k citlivým údajom alebo spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

23.07.2019

CVE

CVE-2019-10972, CVE-2019-10976

Zasiahnuté systémy

Mitsubishi Electric FR Configurator2 verzie staršie ako 1.17T

Následky

Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

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://www.us-cert.gov/ics/advisories/icsa-19-204-01

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

Identifikátor

eClass platform zraniteľnosti

Popis

Vývojári e-learningovej platformy eClass vydali bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injekcie spôsobiť neoprávnené zmeny v systéme alebo získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

25.07.2019

CVE

CVE-2019-9884, CVE-2019-9885

Zasiahnuté systémy

eClass platform verzia staršia ako 2.5.10.2.1

Následky

Neoprávnená zmena v systéme
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.twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?lang=en-US&id=35
https://www.twcert.org.tw/subpages/ServeThePublic/public_document_details.aspx?lang=en-US&id=34
https://exchange.xforce.ibmcloud.com/vulnerabilities/164268
https://exchange.xforce.ibmcloud.com/vulnerabilities/164269

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

Identifikátor

Poppler zraniteľnosť

Popis

Vývojári knižnice PDF Poppler vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii JPXStream::init.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.07.2019

CVE

CVE-2019-9959

Zasiahnuté systémy

Poppler verzie staršie ako 0.79.0

Následky

Zneprístupnenie služby

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).

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=60516
https://poppler.freedesktop.org/
https://gitlab.freedesktop.org/poppler/poppler/blob/master/NEWS

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

National Renewable Energy Laboratory (NREL) EnergyPlus zraniteľnosť

Popis

Spoločnosť National Renewable Energy Laboratory (NREL) vydala bezpečnostnú aktualizáciu na svoj produkt EnergyPlus, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi spôsobiť pretečenie zásobníka, spôsobiť neoprávnené zmeny v systéme a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

24.07.2019

CVE

CVE-2019-10974

Zasiahnuté systémy

NREL EnergyPlus verzie staršie ako 9.0.1

Následky

Vykonanie škodlivého kódu
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého 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.us-cert.gov/ics/advisories/icsa-19-204-02
https://github.com/NREL/EnergyPlus/releases/tag/v9.0.1