BEZPEČNOSTNÝ BULLETIN

Týždeň 26. 06. 2019 - 02. 07. 2019

OBSAH BEZPEČNOSTNÉHO BULLETINU

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-179

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

Identifikátor

libvirt zraniteľnosti

Popis

Vývojári libvirt vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostné zraniteľnosti v API rozhraní.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.06.2019

CVE

CVE-2019-10161, CVE-2019-10166, CVE-2019-10167, CVE-2019-10168

Zasiahnuté systémy

libvirt verzie staršie ako 4.10.1 a 5.4.1

Následky

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

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.

Zdroje

https://access.redhat.com/errata/RHSA-2019:1580
https://tools.cisco.com/security/center/viewAlert.x?alertId=60386
https://tools.cisco.com/security/center/viewAlert.x?alertId=60387
https://tools.cisco.com/security/center/viewAlert.x?alertId=60388
https://tools.cisco.com/security/center/viewAlert.x?alertId=60389
https://www.securityfocus.com/bid/108871/info
https://libvirt.org/git/?p=libvirt.git;a=commit;h=aed6a032cead4386472afb24b16196579e239580

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

Identifikátor

Quadbase EspressReport ES (ERES) zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostných zraniteľnostiach v analytickom software Quadbase EspressReport ES (ERES).
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.06.2019

CVE

CVE-2019-9957, CVE-2019-9958

Zasiahnuté systémy

Quadbase EspressReports ES Version 7 Update 7

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu.
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://exchange.xforce.ibmcloud.com/vulnerabilities/162867
https://exchange.xforce.ibmcloud.com/vulnerabilities/162864
https://crawl3r.xyz/cve/cve-2019-9958/

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

Identifikátor

ABB P610 Panel Builder 600 zraniteľnosti

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na svoj produkt P610 Panel Builder 60, ktoré opravujú bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

27.06.2019

CVE

CVE-2019-7225, CVE-2019-7226, CVE-2019-7227, CVE-2019-7228, CVE-2019-7230, CVE-2019-7231, CVE-2019-7232

Zasiahnuté systémy

PB610 Panel Builder 600 verzie staršie ako 2.8.0.424
Board support package UN30 a UN31 verzie staršie ako 2.31

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup do systému

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-19-178-01

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

Identifikátor

ABB CP635 HMI a ABB CP 651 HMI zraniteľnosti

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na svoje kontrolné panely CP635 HMI a ABB CP 651 HMI, ktoré opravujú bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti spočívajú v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňujú vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.06.2019

CVE

CVE-2019-10995, CVE-2019-7225

Zasiahnuté systémy

ABB CP635 HMI CP620, order code: 1SAP520100R0001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP620, order code: 1SAP520100R4001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP630, order code: 1SAP530100R0001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP635, order code: 1SAP535100R0001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP635, order code: 1SAP535100R5001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP635-B, order code: 1SAP535100R2001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP635-WEB, order code: 1SAP535200R0001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP630-WEB, order code: 1SAP530200R0001, revision index G1 s BSP UN31 verzie 1.76 a staršie
ABB CP635 HMI CP620-WEB, order code: 1SAP520200R0001, revision index G1 s BSP UN31 verzie 1.76 a staršie
CP651, order code: 1SAP551100R0001, revision index B1 s BSP UN30 v1.76 a staršie
CP661, order code: 1SAP561100R0001, revision index B1 s BSP UN30 v1.76 a staršie
CP665, order code: 1SAP565100R0001, revision index B1 s BSP UN30 v1.76 a staršie
CP676, order code: 1SAP576100R0001, revision index B1 s BSP UN30 v1.76 a staršie
CP661-WEB, order code: 1SAP561200R0001, revision index A0 s BSP UN30 v1.76 a staršie
CP651-WEB, order code: 1SAP551200R0001, revision index A0 s BSP UN30 v1.76 a staršie
CP665-WEB, order code: 1SAP565200R0001, revision index A0 s BSP UN30 v1.76 a staršie
CP676-WEB, order code: 1SAP576200R0001, revision index A0 s BSP UN30 v1.76 a staršie

Následky

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

Odporúčania

Administrátorom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, 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.
Administrátorom 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.us-cert.gov/ics/advisories/icsa-19-178-03
https://www.us-cert.gov/ics/advisories/icsa-19-178-02

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

Identifikátor

IBM Db2 zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoj produkt Db2, ktoré opravujú bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.06.2019

CVE

CVE-2019-4057, CVE-2019-4101, CVE-2019-4102, CVE-2019-4154, CVE-2019-4322, CVE-2019-4386

Zasiahnuté systémy

IBM DB2 verzie staršie než Special Build 9.7 FP11
IBM DB2 verzie staršie než Special Build 10.1 FP6
IBM DB2 verzie staršie než Special Build 10.5 FP10
IBM DB2 verzie staršie než Special Build 11.1.4.4 iFix001

Následky

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

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10884444
https://www-01.ibm.com/support/docview.wss?uid=ibm10880737
https://www-01.ibm.com/support/docview.wss?uid=ibm10880735
https://www-01.ibm.com/support/docview.wss?uid=ibm10886809
https://www-01.ibm.com/support/docview.wss?uid=ibm10880741
https://www-01.ibm.com/support/docview.wss?uid=ibm10880743

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Spectrum Protect Plus zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Spectrum Protect Plus, ktorá opravuje bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.06.2019

CVE

CVE-2019-4357, CVE-2019-4383

Zasiahnuté systémy

IBM Spectrum Protect Plus verzie staršie ako 10.1.4

Následky

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

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.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10886111
https://exchange.xforce.ibmcloud.com/vulnerabilities/161667
https://exchange.xforce.ibmcloud.com/vulnerabilities/162165

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

Identifikátor

cURL libcurl zraniteľnosť

Popis

Vývojári nástroja cUrl (libcurl) vydali bezpečnostnú aktualizáciu, ktorá opravuje viacero chýb a bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v OpenSSL engine je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

24.06.2019

CVE

CVE-2019-5443

Zasiahnuté systémy

cURL libcurl pre Windows verzie staršie ako 7.65.1_2

Následky

Vykonanie škodlivého kódu

Odporúčania

Administrátorom odporúčame bezodkladne 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 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://exchange.xforce.ibmcloud.com/vulnerabilities/162844
https://curl.haxx.se/docs/CVE-2019-5443.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM Robotic Process Automation zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt Robotic Process Automation, ktorá opravuje bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá.

Dátum prvého zverejnenia varovania

28.06.2019

CVE

CVE-2019-4295, CVE-2019-4296, CVE-2019-4297, CVE-2019-4298, CVE-2019-4299, CVE-2019-4336, CVE-2019-4337

Zasiahnuté systémy

IBM Robotic Process Automation with Automation Anywhere verzie staršie ako 11.0.0.5

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://www-01.ibm.com/support/docview.wss?uid=ibm10884820
https://www-01.ibm.com/support/docview.wss?uid=ibm10884848
https://www-01.ibm.com/support/docview.wss?uid=ibm10884826
https://www-01.ibm.com/support/docview.wss?uid=ibm10884850
https://www-01.ibm.com/support/docview.wss?uid=ibm10884842
https://www-01.ibm.com/support/docview.wss?uid=ibm10884840
https://www-01.ibm.com/support/docview.wss?uid=ibm10884844

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

Identifikátor

Zraniteľnosť inzulínových púmp Medtronic MiniMed 508 a Paradigm Series

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti v inzulínových pumpách Medtronic MiniMed 508 a Paradigm Series.
Bezpečnostná zraniteľnosť v rádio-frekvenčnom komunikačnom protokole je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonávať neoprávnené zmeny v systéme a získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

27.06.2019

CVE

CVE-2019-10964

Zasiahnuté systémy

Medtronic MiniMed 508 pumpy všetky verzie
Medtronic MiniMed Paradigm 511 pumpy všetky verzie
Medtronic MiniMed Paradigm 512/712 pumpy všetky verzie
Medtronic MiniMed Paradigm 712E pumpy všetky verzie
Medtronic MiniMed Paradigm 515/715 pumpy všetky verzie
Medtronic MiniMed Paradigm 522/722 pumpy všetky verzie
Medtronic MiniMed Paradigm 522K/722K pumpy všetky verzie
Medtronic MiniMed Paradigm 523/723 pumpy verzie staršie ako 2.4A
Medtronic MiniMed Paradigm 523K/723K pumpy verzie staršie ako 2.4A
Medtronic MiniMed Paradigm Veo 554/754 pumpy verzie staršie ako 2.6A
Medtronic MiniMed Paradigm Veo 554/754CM pumpy verzie staršie ako 2.7A

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Výrobca o zraniteľnosti informoval a zraniteľné zariadenia vymieňa za novšie modely. Pre bližšie informácie Vám odporúčame obrátiť sa na distribútora Vášho zariadenia.
Taktiež odporúčame nepripájať zraniteľné inzulínové pumpy do zariadení tretích strán a tiež odpájať komunikačný modul CareLink USB, keď nie je používaný.

Zdroje

https://www.us-cert.gov/ics/advisories/icsma-19-178-01
https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication
https://www.securityfocus.com/bid/108926/info
https://www.theregister.co.uk/2019/06/28/medtronic_insulin_pump_recall/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Arlo Basestation zraniteľnosti

Popis

Spoločnosť Arlo vydala bezpečnostné aktualizácie na svoje základňové stanice pre kamery, ktoré opravujú bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočnou implementáciou bezpečnostných mechanizmov a existenciou zabudovaného používateľského účtu s predvoleným heslom. Zraniteľnosti umožňujú lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu získať kontrolu nad systémom.

Dátum prvého zverejnenia varovania

01.07.2019

CVE

CVE-2019-3949, CVE-2019-3950

Zasiahnuté systémy

Arlo Basestation VMB3010 a VMB4000 verzie staršie ako 1.12.2.3_2782
Arlo Basestation VMB3500 a VMB4500 verzie staršie ako 1.12.2.4_2773
Arlo Basestation VMB5000 verzie staršie ako 1.12.2.3_59_4a57cce

Následky

Neoprávnený prístup do systému
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Administrátorom odporúčame limitovať prístup k administratívnemu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://kb.arlo.com/000062274/Security-Advisory-for-Networking-Misconfiguration-and-Insufficient-UART-Protection-Mechanisms
https://www.tenable.com/security/research/tra-2019-30

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Kubernetes kubectl zraniteľnosť

Popis

Vývojári Kubernetes vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v komponente kubectl.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

20.06.2019

CVE

CVE-2019-11246

Zasiahnuté systémy

Kubernetes kubectl verzie staršie ako 1.12.9
Kubernetes kubectl verzie staršie ako 1.13.6
Kubernetes kubectl verzie staršie ako 1.14.2

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://access.redhat.com/security/cve/cve-2019-11246
https://www.infosecurity-magazine.com/news/incomplete-fix-leads-to-new-1-1/
https://seclists.org/oss-sec/2019/q2/194
https://github.com/kubernetes/kubernetes/pull/76788