BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 02. 2021 - 16. 02. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Bezpečnostná zraniteľnosť v produkte Connman	Vysoká	**8.8**
02.	Viacero bezpečnostných zraniteľností v produktoch Intel	Vysoká	**8.8**
03.	Kritická bezpečnostná zraniteľnosť v produktoch Adobe	Vysoká	**7.8**
04.	Bezpečnostná zraniteľnosť v Linux Kernel	Vysoká	**7.8**
05.	Bezpečnostná zraniteľnosť v produkte Firejail	Vysoká	**7.8**
06.	Bezpečnostná zraniteľnosť v produkte ABB AC500 V2 Webserver	Vysoká	**7.5**
07.	Bezpečnostná zraniteľnosť v produkte Apache Ambari	Vysoká	**7.5**
08.	Bezpečnostná zraniteľnosť v produkte Open vSwitch	Vysoká	**7.5**
09.	Bezpečnostná zraniteľnosť v produktoch Rockwell Automation	Vysoká	**7.5**
10.	Bezpečnostná zraniteľnosť v produkte VMware VSphere Replication	Vysoká	**7.2**
11.	Bezpečnostná zraniteľnosť v produkte LinkedIn Oncall	Vysoká	**7.2**
12.	Dve bezpečnostné zraniteľnosti v produktoch GE Digital	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:
01439/2020/SK-CERT-330

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Connman

Popis

Vývojári linuxového démona Connman vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.02.2021

CVE

CVE-2021-26675

Zasiahnuté systémy

Connman vo verzii staršej ako 1.39

Následky

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/196375
https://seclists.org/oss-sec/2021/q1/118
https://git.kernel.org/pub/scm/network/connman/connman.git/commit/?id=e4079a20f617a4b076af503f6e4e8b0304c9f2cb
https://01.org/connman

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Intel

Popis

Spoločnosť Intel vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.02.2021

CVE

CVE-2020-0521, CVE-2020-0544, CVE-2020-12361, CVE-2020-12362, CVE-2020-12373, CVE-2020-12377, CVE-2020-24450

Zasiahnuté systémy

Intel Graphics Drivers pre Windows vo verzii staršej ako 15.33.51.5146
Intel Graphics Drivers pre Windows vo verzii staršej ako 15.36.39.5145
Intel Graphics Drivers pre Windows vo verzii staršej ako 15.40.46.5144
Intel Graphics Drivers pre Windows vo verzii staršej ako 15.45.32.5164
Intel Graphics Drivers pre Windows vo verzii staršej ako 26.20.100.8141
Intel Graphics Drivers pre Windows vo verzii staršej ako 27.20.100.8587
Intel Graphics Drivers pre Linux Kernel vo verzii staršej ako 5.5.
Intel Server Board séria S2600ST
Intel Server Board séria S2600BP
Intel Server Board séria S2600WF
Intel Server System R1000WF

Následky

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

Odporúčania

Administrátorom a používateľom 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.

Zdroje

https://threatpost.com/intel-graphics-driver-flaws/163810/
https://exchange.xforce.ibmcloud.com/vulnerabilities/196558
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00369.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00438.html
https://blogs.intel.com/technology/2021/02/ipas-security-advisories-for-february-2021/#gs.t77kli

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

Identifikátor

Kritická bezpečnostná zraniteľnosť v produktoch Adobe

Popis

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností, z toho jednu kritickú.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného dokumentu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Jedna zo zraniteľností je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

10.02.2021

CVE

CVE-2021-21012, CVE-2021-21013, CVE-2021-21014, CVE-2021-21015, CVE-2021-21016, CVE-2021-21017, CVE-2021-21018, CVE-2021-21019, CVE-2021-21020, CVE-2021-21021, CVE-2021-21022, CVE-2021-21023, CVE-2021-21024, CVE-2021-21025, CVE-2021-21026, CVE-2021-21027, CVE-2021-21028, CVE-2021-21029, CVE-2021-21030, CVE-2021-21031, CVE-2021-21032, CVE-2021-21033, CVE-2021-21034, CVE-2021-21035, CVE-2021-21037, CVE-2021-21038, CVE-2021-21039, CVE-2021-21040, CVE-2021-21041, CVE-2021-21042, CVE-2021-21044, CVE-2021-21045, CVE-2021-21046, CVE-2021-21047, CVE-2021-21048, CVE-2021-21049, CVE-2021-21050, CVE-2021-21051, CVE-2021-21052, CVE-2021-21053, CVE-2021-21054, CVE-2021-21055, CVE-2021-21057, CVE-2021-21058, CVE-2021-21059, CVE-2021-21060, CVE-2021-21061, CVE-2021-21062, CVE-2021-21063

Zasiahnuté systémy

Adobe Photoshop 2020 vo verzii staršej ako 21.2.5
Adobe Photoshop 2021 vo verzii staršej ako 22.2
Adobe Dreamweaver vo verzii staršej ako 20.2.1 and 21.1
Acrobat DC and Reader DC vo verzii staršej ako 2021.001.20135
Acrobat 2020 and Acrobat Reader 2020 vo verzii staršej ako 2020.001.30020
Acrobat 2017 and Acrobat Reader 2017 vo verzii staršej ako 2017.011.30190
Adobe Animate vo verzii staršej ako21.0.3
Adobe Illustrator vo verzii staršej ako 25.2
Magento Commerce and Open Source vo verzii staršej ako 2.4.2
Magento Commerce and Open Source vo verzii staršej ako 2.4.1-p1
Magento Commerce and Open Source vo verzii staršej ako 2.3.6-p1

Následky

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

Odporúčania
Administrátorom a používateľom 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. 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-products-could-allow-for-arbitrary-code-execution_2021-025/ https://threatpost.com/critical-adobe-windows-flaw/163789/ https://www.securityweek.com/adobe-patches-reader-vulnerability-exploited-wild https://exchange.xforce.ibmcloud.com/vulnerabilities/196196 https://www.thezdi.com/blog/2021/2/9/the-february-2022-security-update-review https://www.helpnetsecurity.com/2021/02/09/february-2021-patch-tuesday/

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

Identifikátor

Bezpečnostná zraniteľnosť v Linux Kernel

Popis

Vývojári Kernelu operačného systému Linux vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov eskalovať svoje privilégiá na systéme.

Dátum prvého zverejnenia varovania

05.02.2021

CVE

CVE-2021-26708

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 5.10.13

Následky

Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/196316
https://seclists.org/oss-sec/2021/q1/113
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c518adafa39f37858697ac9309c6cf1805581446

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Firejail

Popis

Vývojári sandboxu Firejail vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.02.2021

CVE

CVE-2021-26910

Zasiahnuté systémy

Firejail vo verzii staršej ako 0.9.64.4

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/196411
https://unparalleled.eu/publications/2021/advisory-unpar-2021-0.txt
https://firejail.wordpress.com/

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte ABB AC500 V2 Webserver

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na produkty série AC500, ktoré opravujä bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.02.2021

CVE

CVE-2020-24686

Zasiahnuté systémy

AC500 V2 PM554 všetky verzie
AC500 V2 PM556 všetky verzie
AC500 V2 PM564 všetky verzie
AC500 V2 PM566 všetky verzie
AC500 V2 PM572 všetky verzie
AC500 V2 PM573 všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://search.abb.com/library/Download.aspx?DocumentID=3ADR010645&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.82863570.570457735.1612853065-1820210962.1612853065

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Apache Ambari

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Ambari, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

07.02.2021

CVE

CVE-2020-13924

Zasiahnuté systémy

Apache Ambari vo verzii staršej ako 2.7.5

Následky

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://exchange.xforce.ibmcloud.com/vulnerabilities/196372
https://seclists.org/oss-sec/2021/q1/116
https://ambari.apache.org/whats-new.html

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Open vSwitch

Popis

Vývojári programu Open vSwitch vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.02.2021

CVE

CVE-2020-35498

Zasiahnuté systémy

Open vSwitch vo verzii staršej ako 2.14.2
Open vSwitch vo verzii staršej ako 2.13.3
Open vSwitch vo verzii staršej ako 2.12.3
Open vSwitch vo verzii staršej ako 2.11.6
Open vSwitch vo verzii staršej ako 2.10.7
Open vSwitch vo verzii staršej ako 2.9.9
Open vSwitch vo verzii staršej ako 2.8.11
Open vSwitch vo verzii staršej ako 2.7.13
Open vSwitch vo verzii staršej ako 2.6.10
Open vSwitch vo verzii staršej ako 2.5.12

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/196600
https://seclists.org/oss-sec/2021/q1/135
https://github.com/openvswitch/ovs/commit/79349cbab0b2a755140eedb91833ad2760520a83
https://www.sdxcentral.com/open-source/definitions/what-is-open-vswitch/

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

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Rockwell Automation

Popis

Spoločnosť Rockwell Automation vydala bezpečnostné aktualizácie na svoje produkty DriveTools SP a Drives AOP, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá, získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.02.2021

CVE

CVE-2021-22665

Zasiahnuté systémy

DriveTools vo verzii staršej ako SP v5.14.41
Drives AOP vo verzii staršej ako v4.13.41

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace systémy a jednotky odporúčame prevádzkovať úplne oddelené od Internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://us-cert.cisa.gov/ics/advisories/icsa-21-042-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte VMware VSphere Replication

Popis

Spoločnosť VMware vydala bezpečnostné aktualizácie na produkt VMware VSphere Replication, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.02.2021

CVE

CVE-2021-21976

Zasiahnuté systémy

vSphere Replication vo verzii staršej ako 8.3.1.2
vSphere Replication vo verzii staršej ako 8.2.1.1
vSphere Replication vo verzii staršej ako 8.1.2.3
vSphere Replication vo verzii staršej ako 6.5.1.5

Následky

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

Odporúčania

Administrátorom a používateľom 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.

Zdroje

https://www.vmware.com/security/advisories/VMSA-2021-0001.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/196646

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte LinkedIn Oncall

Popis

Spoločnosť LinkedIn vydala bezpečnostnú aktualizáciu na svoj produkt Oncall, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

05.02.2021

CVE

CVE-2021-26722

Zasiahnuté systémy

LinkedIn Oncall vo verzii staršej ako 1.4.0 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://exchange.xforce.ibmcloud.com/vulnerabilities/196327
https://github.com/linkedin/oncall/issues/341
https://oncall.tools/

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

Identifikátor

Dve bezpečnostné zraniteľnosti v produktoch GE Digital

Popis

Spoločnosť GE Digital vydala bezpečnostnú aktualizáciu na svoj produkt iFIX, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom modifikácie systémových registrov získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

09.02.2021

CVE

CVE-2019-18243, CVE-2019-18255

Zasiahnuté systémy

GE Digital iFIX vo verzii staršej ako v6.5

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Eskalácia privilégií

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom 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://us-cert.cisa.gov/ics/advisories/icsa-21-040-01