BEZPEČNOSTNÝ BULLETIN

Týždeň 13. 01. 2021 - 19. 01. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Viacero bezpečnostných zraniteľností v produktoch Cisco	Vysoká	**8.8**
02.	Viacero bezpečnostných zraniteľností v nástroji Jenkins	Vysoká	**8.8**
03.	Bezpečnostná zraniteľnosť v produkte Eclipse Hono	Vysoká	**8.8**
04.	Bezpečnostná zraniteľnosť v produkte Nagios XI	Vysoká	**8.8**
05.	Viacero bezpečnostných zraniteľností v produktoch NVIDIA	Vysoká	**8.4**
06.	Dve bezpečnostné zraniteľnosti v produktoch Mitsubishi Electric	Vysoká	**8.3**
07.	Bezpečnostná zraniteľnosť v produkte Apache Tomcat	Vysoká	**8.2**
08.	Bezpečnostná zraniteľnosť v produkte Flatpak	Vysoká	**7.8**
09.	Bezpečnostná zraniteľnosť v produkte Open-iSCSI tcmu-runner	Vysoká	**7.3**

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-306

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 Cisco

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.01.2021

CVE

CVE-2019-15992, CVE-2021-1126, CVE-2021-1127, CVE-2021-1130, CVE-2021-1131, CVE-2021-1143, CVE-2021-1144, CVE-2021-1145, CVE-2021-1146, CVE-2021-1147, CVE-2021-1148, CVE-2021-1149, CVE-2021-1150, CVE-2021-1151, CVE-2021-1152, CVE-2021-1153, CVE-2021-1159, CVE-2021-1160, CVE-2021-1161, CVE-2021-1162, CVE-2021-1163, CVE-2021-1164, CVE-2021-1165, CVE-2021-1166, CVE-2021-1167, CVE-2021-1168, CVE-2021-1169, CVE-2021-1170, CVE-2021-1171, CVE-2021-1172, CVE-2021-1173, CVE-2021-1174, CVE-2021-1175, CVE-2021-1176, CVE-2021-1177, CVE-2021-1178, CVE-2021-1179, CVE-2021-1180, CVE-2021-1181, CVE-2021-1182, CVE-2021-1183, CVE-2021-1184, CVE-2021-1185, CVE-2021-1186, CVE-2021-1187, CVE-2021-1188, CVE-2021-1189, CVE-2021-1190, CVE-2021-1191, CVE-2021-1192, CVE-2021-1193, CVE-2021-1194, CVE-2021-1195, CVE-2021-1196, CVE-2021-1197, CVE-2021-1198, CVE-2021-1199, CVE-2021-1200, CVE-2021-1201, CVE-2021-1202, CVE-2021-1203, CVE-2021-1204, CVE-2021-1205, CVE-2021-1206, CVE-2021-1207, CVE-2021-1208, CVE-2021-1209, CVE-2021-1210, CVE-2021-1211, CVE-2021-1212, CVE-2021-1213, CVE-2021-1214, CVE-2021-1215, CVE-2021-1216, CVE-2021-1217, CVE-2021-1223, CVE-2021-1224, CVE-2021-1226, CVE-2021-1236, CVE-2021-1237, CVE-2021-1238, CVE-2021-1239, CVE-2021-1240, CVE-2021-1242, CVE-2021-1245, CVE-2021-1246, CVE-2021-1258, CVE-2021-1267, CVE-2021-1307, CVE-2021-1310, CVE-2021-1311, CVE-2021-1360

Zasiahnuté systémy

Cisco ASA Software vo verzii staršej ako 9.4
AnyConnect Secure Mobility Client pre Linux vo verzii staršej ako 4.9.03047
AnyConnect Secure Mobility Client pre MacOS vo verzii staršej ako 4.9.03047
AnyConnect Secure Mobility Client pre Windows vo verzii staršej ako 4.9.03049
Cisco CMX Release vo verzii staršej ako 10.6.3
Unified Communications Manager (Unified CM) vo verzii staršej ako 12.5(1)SU3
Unified Communications Manager Session Management Edition (Unified CM SME) vo verzii staršej ako 12.5(1)SU3
Unified Communications Manager IM and Presence Service (Unified CM IMP) vo verzii staršej ako 12.5(1)SU3
Unity Connection vo verzii staršej ako 12.5(1)SU3
Emergency Responder vo verzii staršej ako 12.5(1)SU3
Prime License Manager vo verzii staršej ako 11.5(1)SU9
Cisco DNA Center Software vo verzii staršej ako 2.2.1.0
Cisco FMC vo verzii staršej ako 6.7.0
IP kamery Cisco Video Surveillance 8000 séria s nainštalovaným firmware vo verzii staršej ako 1.0.9-8 a aktívnym Cisco Discovery protokolom
Cisco Finesse vo verzii staršej ako 12.5 ES05
Cisco Enterprise NFVIS zariadenia vo verzii staršej ako 4.4.1
Cisco Proximity Desktop pre Windows vo verzii staršej ako 3.1.0
RV110W Wireless-N VPN Firewall (všetky verzie - ukončená podpora)
RV130 VPN Router (všetky verzie - ukončená podpora)
RV130W Wireless-N Multifunction VPN Router (všetky verzie - ukončená podpora)
RV215W Wireless-N VPN Router (všetky verzie - ukončená podpora)
1000 Series Integrated Services Routers (ISRs) všetky verzie
3000 Series Industrial Security Appliances (ISAs) všetky verzie
4000 Series Integrated Services Routers (ISRs) všetky verzie
Cloud Services Router 1000V všetky verzie
Cisco UTD Snort IPS Engine Software vo verzii staršej ako XE 17.4.1
Firepower Threat Defense (FTD) Software vo verzii staršej ako 6.5.0.5
Snort vo verzii staršej ako2.9.14.10
Integrated Services Virtual Router (ISRv) všetky verzie
Meraki MX64 všetky verzie
Meraki MX64W všetky verzie
Meraki MX67 všetky verzie
Meraki MX67C všetky verzie
Meraki MX67W všetky verzie
Meraki MX68 všetky verzie
Meraki MX68CW všetky verzie
Meraki MX68W všetky verzie
Meraki MX100 všetky verzie
Meraki MX84 všetky verzie
Meraki MX250 všetky verzie
Meraki MX450 všetky verzie
Cisco ASR 5000 séria routerov vo verzii staršej ako 21.19.7
Cisco Webex Meetings stránky vo verzii staršej ako 24.11.2020
Cisco Webex Meetings Server vo verzii staršej ako 3.0MR3 Security Patch 6
Cisco Webex Meetings Server vo verzii staršej ako 4.0MR3 Security Patch 5
Cisco Webex Teams vo verzii staršej ako 40.12.0.17293.
Cisco AnyConnect Secure Mobility Client pre Windows vo verzii staršej ako 4.9.04043
Presnú specifikáciu jednotlivých zasiahnutých produktov nájdete na webovej adrese:
https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities

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://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities https://threatpost.com/cisco-flaw-cmx-software-retailers/163027/

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

Identifikátor

Viacero bezpečnostných zraniteľností v nástroji Jenkins

Popis

Vývojári nástroja Jenkins vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.01.2021

CVE

CVE-2021-21602, CVE-2021-21603, CVE-2021-21604, CVE-2021-21605, CVE-2021-21606, CVE-2021-21607, CVE-2021-21608, CVE-2021-21609, CVE-2021-21610, CVE-2021-21611, CVE-2021-21612, CVE-2021-21613, CVE-2021-21614

Zasiahnuté systémy

Jenkins weekly vo verzii staršej ako 2.275
Jenkins LTS vo verzii staršej ako 2.263.2
Bumblebee HP ALM Plugin vo verzii staršej ako 4.1.6
TICS Plugin vo verzii staršej ako 2020.3.0.7
TraceTronic ECU-TEST vo verzii staršej ako 2.24

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://exchange.xforce.ibmcloud.com/vulnerabilities/194812
https://www.jenkins.io/security/advisory/2021-01-13/

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Eclipse Hono

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Eclipse Hono.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi, prostredníctvom zasielania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.01.2021

CVE

CVE-2020-27220

Zasiahnuté systémy

Eclipse Hono vo verzii staršej ako 1.4.0 (vrátane)
Eclipse Hono vo verzii staršej ako 1.5.0 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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/194972
https://bugs.eclipse.org/bugs/show_bug.cgi?id=569856
https://github.com/eclipse/hono
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27220

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Nagios XI

Popis

Spoločnosť Nagios vydala bezpečnostnú aktualizáciu na svoj produkt Nagios XI, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi, prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.01.2021

CVE

CVE-2020-35578

Zasiahnuté systémy

Nagios XI vo verzii staršej ako 5.8.0

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

Zdroje

https://www.nagios.com/downloads/nagios-xi/change-log/
https://www.exploit-db.com/exploits/49422
https://packetstormsecurity.com/files/160948

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

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch NVIDIA

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na produkty NVIDIA GPU Display Driver a NVIDIA vGPU Software, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégiá a znepristupniť službu.

Dátum prvého zverejnenia varovania

11.01.2021

CVE

-

Zasiahnuté systémy

NVIDIA GPU display drivers pre Windows a Linux
NVIDIA Virtual GPU (vGPU) management software
Presnú specifikáciu jednotlivých zasiahnutých produktov nájdete na stránke:
https://nvidia.custhelp.com/app/answers/detail/a_id/5142

Následky

Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Znepristupnenie služby
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://nvidia.custhelp.com/app/answers/detail/a_id/5142
https://www.secplicity.org/2021/01/12/11-high-severity-vulnerabilities-found-in-nvidia-software/
https://www.bleepingcomputer.com/news/security/nvidia-fixes-high-severity-flaws-affecting-windows-linux-devices/
https://www.techradar.com/news/nvidia-has-patched-several-serious-security-flaws-affecting-windows-and-linux-devices

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.3**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dve bezpečnostné zraniteľnosti v produktoch Mitsubishi Electric

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na produkty Factory Automation, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

14.01.2021

CVE

CVE-2020-14521, CVE-2020-14523

Zasiahnuté systémy
CW Configurator vo verzii staršej ako 1.011M
FR Configurator2 vo verzii staršej ako 1.23Z
GX Works2 vo verzii staršej ako 1.596W
GX Works3 vo verzii staršej ako 1.065T
MELSOFT iQ AppPortal vo verzii staršej ako 1.20W
MELSOFT Navigator vo verzii staršej ako 2.74C
MR Configurator2 vo verzii staršej ako 1.115V
MX Component vo verzii staršej ako 4.21X
MT Works2 vo verzii staršej ako 1.160S
RT ToolBox3 vo verzii staršej ako 1.80J
MELSEC iQ-R Series Motion Module všetky verzie
MI Configurator všetky verzie
C Controller Interface Module Utility všetky verzie
C Controller Module Setting and Monitoring Tool všetky verzie
CC-Link IE Control Network Data Collector všetky verzie
CC-Link IE Field Network Data Collector všetky verzie
CPU Module Logging Configuration Tool vo verzii staršej ako 1.100E (vrátane)
CW Configurator vo verzii staršej ako 1.010L (vrátane)
Data Transfer vo verzii staršej ako 3.42U (vrátane)
EZSocket všetky verzie
FR Configurator SW3 všetky verzie
GT Designer2 Classic všetky verzie
GT Designer3 Version1 (GOT1000) vo verzii staršej ako 1.241B (vrátane)
GT Designer3 Version1 (GOT2000) vo verzii staršej ako 1.241B (vrátane)
GT SoftGOT1000 Version3 vo verzii staršej ako 3.200J (vrátane)
GT SoftGOT2000 Version1 vo verzii staršej ako 1.241B (vrátane)
GX Developer vo verzii staršej ako 8.504A (vrátane)
GX LogViewer vo verzii staršej ako 1.100E (vrátane)
M_CommDTM-IO-Link, all versions
MELFA-Works všetky verzie
MELSEC WinCPU Setting Utility všetky verzie
MELSOFT Complete Clean Up Tool všetky verzie
MELSOFT EM Software Development Kit všetky verzie
Motion Control Setting vo verzii staršej ako 1.005F (vrátane)
Motorizer vo verzii staršej ako 1.005F (vrátane)
MTConnect Data Collector všetky verzie
MX MESInterface vo verzii staršej ako 1.21X (vrátane)
MX MESInterface-R vo verzii staršej ako 1.12N (vrátane)
MX Sheet vo verzii staršej ako 2.15R (vrátane)
Network Interface Board CC IE Control Utility všetky verzie
Network Interface Board CC IE Field Utility všetky verzie
Network Interface Board CC-Link Ver.2 Utility všetky verzie
Network Interface Board MNETH Utility všetky verzie
Position Board utility 2 všetky verzie
PX Developer všetky verzie
RT ToolBox2 všetky verzie
RT ToolBox3 všetky verzie
Setting/monitoring tools pre C Controller modul všetky verzie
SLMP Data Collector všetky verzie

Následky
Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému Neoprávnený prístup k citlivým údajom Neoprávnená zmena v systéme Zneprístupnenie služby

Odporúčania
Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. 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. 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://us-cert.cisa.gov/ics/advisories/icsa-20-212-04 https://us-cert.cisa.gov/ics/advisories/icsa-20-212-03

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Apache Tomcat

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Tomcat, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

14.01.2021

CVE

CVE-2021-24122

Zasiahnuté systémy

Apache Tomcat vo verzii staršej ako 7.0.107
Apache Tomcat vo verzii staršej ako 8.5.60
Apache Tomcat vo verzii staršej ako 9.0.40
Apache Tomcat vo verzii staršej ako 10.0.0-M10

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/194894

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Flatpak

Popis

Vývojári knižnice Flatpak vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
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

14.01.2021

CVE

CVE-2021-21261

Zasiahnuté systémy

Flatpak vo verzii staršej ako 1.10.0
Flatpak vo verzii staršej ako 1.8.5

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://github.com/flatpak/flatpak/security/advisories/GHSA-4ppf-fxf6-vxg2
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21261
https://exchange.xforce.ibmcloud.com/vulnerabilities/194967

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

Identifikátor

Bezpečnostná zraniteľnosť v produkte Open-iSCSI tcmu-runner

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Open-iSCSI tcmu-runner.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

14.01.2021

CVE

CVE-2021-3139

Zasiahnuté systémy

Open-iSCSI tcmu-runner vo verzii staršej ako 1.5.2 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom 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/194936
https://github.com/open-iscsi/tcmu-runner/pull/644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3139