



## OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	V8 JavaScript engine - bezpečnostná zraniteľnosť	Vysoká	8.8
02.	Advantech WebAccessSCADA - bezpečnostná zraniteľnosť	Vysoká	8.8
03.	Schneider Electric SoMachine Basic a C-Bus Toolkit - bezpečnostné zraniteľnosti	Vysoká	8.8
04.	TIBCO Messaging - bezpečnostná zraniteľnosť	Vysoká	8.8
05.	Multilaser Router AC1200 produkt - bezpečnostná zraniteľnosť	Vysoká	8.8
06.	GitLab Workhorse	Vysoká	8.5
07.	EIPStackGroup OpENer Ethernet/IP - bezpečnostné zraniteľnosti	Vysoká	8.2
08.	Adobe produkty - viacero bezpečnostných zraniteľností	Vysoká	7.8
09.	JTEKT TOYOPUC produkty - bezpečnostná zraniteľnosť	Vysoká	7.5
10.	Node.js moduly swiper a chrono-node - dve bezpečnostné zraniteľnosti	Vysoká	7.5
11.	Kubernetes - bezpečnostná zraniteľnosť	Stredná	6.5



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

V8 JavaScript engine - bezpečnostná zraniteľnosť

#### Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti V8 JavaScript renderovacieho enginu používaného vo webových prehliadačoch založených na báze Chromium.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného HTML vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

#### Dátum prvého zverejnenia varovania

12.04.2021

#### CVE

-

#### Zasiahnuté systémy

V8 JavaScript rendering engine vo verzii staršej ako 9.0 (vrátane)

Webové prehliadače založené na báze Chromium

#### Následky

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

#### 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.

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://thehackernews.com/2021/04/rce-exploit-released-for-unpatched.html>

<https://www.bleepingcomputer.com/news/security/google-chrome-microsoft-edge-zero-day-vulnerability-shared-on-twitter/>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

Advantech WebAccessSCADA - bezpečnostná zraniteľnosť

#### Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt WebAccessSCADA, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi eskalovať svoje privilégia a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

#### Dátum prvého zverejnenia varovania

13.04.2021

#### CVE

CVE-2021-22669

#### Zasiahnuté systémy

Advantech WebAccessSCADA vo verzii staršej ako 9.0.3

#### Následky

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

#### Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

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-21-103-02>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

**Identifikátor**

Schneider Electric SoMachine Basic a C-Bus Toolkit - bezpečnostné zraniteľnosti

**Popis**

Spoločnosť Schneider Electric vydala bezpečnostné aktualizácie na svoje produkty SoMachine Basic a C-Bus Toolkit, 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**

15.04.2021

**CVE**

CVE-2018-7783, CVE-2021-22716, CVE-2021-22717, CVE-2021-22718, CVE-2021-22719, CVE-2021-22720

**Zasiahnuté systémy**

Schneider Electric SoMachine Basic verzie staršie ako v1.6 SP1  
C-Bus Toolkit verzie staršie ako v1.15.7

**Následky**

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

**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 jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu.

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-21-103-01><https://us-cert.cisa.gov/ics/advisories/icsa-21-105-01>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

**Identifikátor**

TIBCO Messaging - bezpečnostná zraniteľnosť

**Popis**

Spoločnosť TIBCO vydala bezpečnostnú aktualizáciu na svoj produkt Messaging, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

**Dátum prvého zverejnenia varovania**

14.04.2021

**CVE**

CVE-2021-28825, CVE-2021-28826

**Zasiahnuté systémy**

TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Community Edition vo verzii staršej ako 2.0.7

TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Enterprise Edition vo verzii staršej ako 2.0.7

**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/200062><https://www.tibco.com/support/advisories/2021/04/tibco-security-advisory-april-14-2021-tibco-messaging-2021-28825>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

Multilaser Router AC1200 produkt - bezpečnostná zraniteľnosť

#### Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Multilaser Router AC1200. Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

#### Dátum prvého zverejnenia varovania

15.04.2021

#### CVE

CVE-2021-31152

#### Zasiahnuté systémy

Multilaser Router AC1200 vo verzii staršej ako 02.03.01.45\_pt (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.

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/199983>

<https://www.youtube.com/watch?v=zN3DVrcu6Eg>

<https://www.multilaser.com.br/>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

GitLab Workhorse

#### Popis

Vývojári programu GitLab Workhorse vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

#### Dátum prvého zverejnenia varovania

11.04.2021

#### CVE

CVE-2021-22190

#### Zasiahnuté systémy

GitLab Workhorse vo verzii staršej ako 13.7.8

GitLab Workhorse vo verzii staršej ako 13.8.5

GitLab Workhorse vo verzii staršej ako 13.9.2

#### Následky

Neoprávnený prístup k citlivým údajom

Neoprávnená zmena v systéme

Zneprístupnenie služby

#### Odporúčania

Administrátorom a používateľom 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.

#### Zdroje

<https://exchange.xforce.ibmcloud.com/vulnerabilities/199766>

<https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22190.json>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.2
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

EIPStackGroup OpENer Ethernet/IP - bezpečnostné zraniteľnosti

#### Popis

Vývojári knižnice EIPStackGroup vydali bezpečnostnú aktualizáciu svojho produktu OpENer, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného balíka spôsobiť zneprístupnenie služby.

#### Dátum prvého zverejnenia varovania

20.04.2015

#### CVE

CVE-2021-27478, CVE-2021-27482, CVE-2021-27498, CVE-2021-27500

#### Zasiahnuté systémy

EIPStackGroup OpENer komity a verzie vydané pred 10. februárom 2021

#### Následky

Zneprístupnenie služby

Neoprávnený prístup k citlivým údajom

#### Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Riadiace jednotky a systémy 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-21-105-02>





Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.8
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

**Identifikátor**

Adobe produkty - viacero bezpečnostných zraniteľností

**Popis**

Spoločnosť Adobe vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

**Dátum prvého zverejnenia varovania**

13.04.2021

**CVE**

CVE-2021-21070, CVE-2021-21091, CVE-2021-21092, CVE-2021-21093, CVE-2021-21094, CVE-2021-21095, CVE-2021-21096, CVE-2021-21100, CVE-2021-28548, CVE-2021-28549

**Zasiahnuté systémy**

Adobe Bridge vo verzii staršej ako 10.1.2  
Adobe Bridge vo verzii staršej ako 11.0.2  
Adobe Photoshop vo verzii staršej ako 21.2.7  
Adobe Photoshop vo verzii staršej ako 22.3.1  
Adobe Digital Editions vo verzii staršej ako 4.5.11.187606  
Adobe RoboHelp vo verzii staršej ako RH2020.0.4

**Následky**

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

**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. 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/adobe-patches-critical-security-holes-bridge-photoshop/165371/>  
<https://www.securityweek.com/adobe-patches-critical-code-execution-vulnerabilities-photoshop-bridge>  
<https://exchange.xforce.ibmcloud.com/vulnerabilities/199822>  
<https://exchange.xforce.ibmcloud.com/vulnerabilities/199831>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

JTEKT TOYOPUC produkty - bezpečnostná zraniteľnosť

#### Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktov JTEKT TOYOPUC. Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

#### Dátum prvého zverejnenia varovania

13.04.2021

#### CVE

CVE-2021-27458

#### Zasiiahnuté systémy

TOYOPUC-PC10 Series PC10G-CPU TCC-6353 všetky verzie  
TOYOPUC-PC10 Series PC10GE TCC-6464 všetky verzie  
TOYOPUC-PC10 Series PC10P TCC-6372 všetky verzie  
TOYOPUC-PC10 Series PC10P-DP TCC-6726 všetky verzie  
TOYOPUC-PC10 Series PC10P-DP-IO TCC-6752 všetky verzie  
TOYOPUC-PC10 Series PC10B-P TCC-6373 všetky verzie  
TOYOPUC-PC10 Series PC10B TCC-1021 všetky verzie  
TOYOPUC-PC10 Series PC10B-E/C TCU-6521 všetky verzie  
TOYOPUC-PC10 Series PC10E TCC-4737 všetky verzie  
TOYOPUC-Plus Series Plus CPU TCC-6740 všetky verzie  
TOYOPUC-Plus Series Plus EX TCU-6741 všetky verzie  
TOYOPUC-Plus Series Plus EX2 TCU-6858 všetky verzie  
TOYOPUC-Plus Series Plus EFR TCU-6743 všetky verzie  
TOYOPUC-Plus Series Plus EFR2 TCU-6859 všetky verzie  
TOYOPUC-Plus Series Plus 2P-EFR TCU-6929 všetky verzie  
TOYOPUC-Plus Series Plus BUS-EX TCU-6900 všetky verzie  
TOYOPUC-PC3J/PC2J Series FL/ET-T-V2H THU-6289 všetky verzie  
TOYOPUC-PC3J/PC2J Series 2PORT-EFR THU-6404 všetky verzie

#### Následky

Zneprístupnenie služby

#### Odporúčania

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od Internetu. Administrátorom odporúčame postupovať podľa návodu zverejnenom na adrese <https://us-cert.cisa.gov/ics/advisories/icsa-21-103-03>



**Zdroje**

<https://us-cert.cisa.gov/ics/advisories/icsa-21-103-03>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 7.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

Node.js moduly swiper a chrono-node - dve bezpečnostné zraniteľnosti

#### Popis

Vývojári modulov swiper a chrono-node pre Node.js vydali bezpečnostné aktualizácie svojich produktov, ktorá opravujú dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

#### Dátum prvého zverejnenia varovania

11.04.2021

#### CVE

CVE-2021-23370, CVE-2021-23371

#### Zasiiahnuté systémy

Node.js swiper vo verzii staršej ako 6.5.1

Node.js chrono-node vo verzii staršej ako 2.2.4

#### Následky

Zneprístupnenie služby

#### Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú vyššie uvedené pluginy v zraniteľných verziách. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

#### Zdroje

<https://exchange.xforce.ibmcloud.com/vulnerabilities/199769>

<https://exchange.xforce.ibmcloud.com/vulnerabilities/199770>

<https://snyk.io/vuln/SNYK-JS-SWIPER-1088062>

<https://www.npmjs.com/package/swiper>

<https://snyk.io/vuln/SNYK-JS-CHRONONODE-1083228>



Dôležitosť	<input type="checkbox"/> Nízka	<input checked="" type="checkbox"/> Stredná	<input type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 6.5
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(CLEAR)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

#### Identifikátor

Kubernetes - bezpečnostná zraniteľnosť

#### Popis

Vývojári kontajnerového systému Kubernetes vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služby.

#### Dátum prvého zverejnenia varovania

14.04.2021

#### CVE

CVE-2021-20291

#### Zasiahnuté systémy

Kubernetes vo verzii staršej ako 1.28.1

CRI-O vo verzii staršej ako v1.20.2

Podman vo verzii staršej ako 3.1.0.

#### Následky

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.

#### Zdroje

<https://threatpost.com/security-bug-brick-kubernetes-clusters/165413/>

<https://cve.circl.lu/cve/CVE-2021-20291>