



OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Bezpečnostné zraniteľnosti v produktoch Apache Druid a Shiro	Vysoká	8.8
02.	Bezpečnostná zraniteľnosť v produktoch Siemens SIMATIC	Vysoká	8.1
03.	Bezpečnostná zraniteľnosť v produkte Docker	Vysoká	8.0
04.	Bezpečnostná zraniteľnosť v produktoch Tibco	Vysoká	8.0
05.	Bezpečnostná zraniteľnosť v produkte Trend Micro Apex One	Vysoká	7.8
06.	Bezpečnostná zraniteľnosť v produktoch Traccar	Vysoká	7.8
07.	Bezpečnostná zraniteľnosť v produkte Horner Automation	Vysoká	7.8
08.	Viacero bezpečnostných zraniteľností v produktoch Luxion	Vysoká	7.8



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(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Bezpečnostné zraniteľnosti v produktoch Apache Druid a Shiro

Popis

Spoločnosť Apache vydala bezpečnostné aktualizácie na svoje produkty Druid a Shiro, ktoré opravujú dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne upravenej žiadosti vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.02.2021

CVE

CVE-2020-17523, CVE-2021-25646

Zasiiahnuté systémy

Apache Druid vo verzii staršej ako 0.20.1

Apache Shiro vo verzii staršej ako 1.7.1

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://meterpreter.org/cve-2021-25646-apache-druid-remote-code-execution-vulnerability-alert/><https://meterpreter.org/cve-2020-17523-apache-shiro-authentication-bypass-vulnerability-alert/><https://cve.circl.lu/cve/CVE-2021-25646><https://nvd.nist.gov/vuln/detail/CVE-2021-25646><https://exchange.xforce.ibmcloud.com/vulnerabilities/195875>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.1
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Siemens SIMATIC

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje produkty SIMATIC HMI Comfort Panel a SIMATIC HMI KTP Mobile Panels, ktoré opravujú bezpečnostnú zraniteľnosť. 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

02.02.2021

CVE

CVE-2020-15798

Zasiahnuté systémy

SIMATIC HMI Comfort Panel (vrátane variantov SIPLUS variants) vo verzii staršej ako v16 Update 3a
SIMATIC HMI KTP Mobile Panels vo verzii staršej ako v16 Update 3a

Následky

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

Odporúčania

Administrátorom 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-21-033-02>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.0
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte Docker

Popis

Vývojári platformy Docker vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zasielania špeciálne upravených paketov eskalovať svoje privilégia a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.02.2021

CVE

CVE-2021-21284

Zasiahnuté systémy

Docker vo verzii staršej ako 19.03.15

Docker vo verzii staršej ako 20.10.3

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://exchange.xforce.ibmcloud.com/vulnerabilities/196047>

<https://github.com/moby/moby/security/advisories/GHSA-7452-xqpi-6rpc>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21284>



Dôležitosť	<input type="checkbox"/> Nízka	<input type="checkbox"/> Stredná	<input checked="" type="checkbox"/> Vysoká	<input type="checkbox"/> Kritická	CVSS skóre: 8.0
Klasifikácia	<input checked="" type="checkbox"/> Neutajované / TLP(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Tibco

Popis

Spoločnosť Tibco vydala bezpečnostnú aktualizáciu na svoj produkt EBX, ktorá opravuje bezpečnostnú zraniteľnosť.

Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať XSS útok a následne získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

02.02.2021

CVE

CVE-2021-23271

Zasiiahnuté systémy

TIBCO EBX vo verzii staršej ako 5.9.13

Následky

Vykonanie škodlivého kódu

Neoprávnený prístup k citlivým údajom

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://exchange.xforce.ibmcloud.com/vulnerabilities/196070>

<https://www.tibco.com/support/advisories/2021/02/tibco-security-advisory-february-2-2021-tibco-ebx>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23271>



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(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte Trend Micro Apex One

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt Micro Apex One, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi eskalovať svoje privilégia a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.01.2021

CVE

CVE-2021-25249

Zasiiahnuté systémy

Trend Micro Apex One On Premise vo verzii staršej ako CP9167

Trend Micro Apex One SaaS vo verzii staršej ako 202101

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://exchange.xforce.ibmcloud.com/vulnerabilities/195845>

<https://success.trendmicro.com/solution/000284202>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25249>

<https://www.zerodayinitiative.com/advisories/ZDI-21-119/>



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(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produktoch Traccar

Popis

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

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

02.02.2021

CVE

CVE-2021-21292

Zasiahnuté systémy

Traccar pre Windows vo verzii staršej ako 4.12

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://exchange.xforce.ibmcloud.com/vulnerabilities/196066>

<https://github.com/traccar/traccar/security/advisories/GHSA-j75r-7qm5-62q5>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21292>



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(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Bezpečnostná zraniteľnosť v produkte Horner Automation

Popis

Spoločnosť Horner Automation vydala bezpečnostnú aktualizáciu na svoj produkt Cscape, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

04.02.2021

CVE

CVE-2021-22663

Zasiahnuté systémy

Cscape vo verzii staršej ako 9.90 SP3.5

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-21-035-02>



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(WHITE)		<input type="checkbox"/> Vyhradené	<input type="checkbox"/> Dôverné	<input type="checkbox"/> Tajné
Kód sektora (dopad)					

Identifikátor

Viacero bezpečnostných zraniteľností v produktoch Luxion

Popis

Spoločnosť Luxion vydala bezpečnostné aktualizácie na svoje produkty KeyShot, ktoré opravujú viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.02.2021

CVE

CVE-2021-22643, CVE-2021-22645, CVE-2021-22647, CVE-2021-22649, CVE-2021-22651

Zasiahnuté systémy

KeyShot versions vo verzii staršej ako 10.1
KeyShot Viewer vo verzii staršej ako 10.1
KeyShot Network Rendering vo verzii staršej ako 10.1
KeyVR vo verzii staršej ako 10.1

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://us-cert.cisa.gov/ics/advisories/icsa-21-035-01>