BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 03. 2021 - 16. 03. 2021

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Siemens produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Emerson Smart Wireless Gateway - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
03.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Madge - bezpečnostná zraniteľnosť	Vysoká	**8.6**
05.	IBM DB2 - dve bezpečnostné zraniteľnosti	Vysoká	**8.4**
06.	TIBCO Spotfire - bezpečnostná zraniteľnosť	Vysoká	**8.0**
07.	Adobe produkty - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
08.	Apache Oozie - bezpečnostná zraniteľnosť	Vysoká	**7.8**
09.	Schneider Electric IGSS SCADA - viacero zraniteľností	Vysoká	**7.8**
10.	Swagger Codegen - bezpečnostná zraniteľnosť	Vysoká	**7.8**
11.	I-net Clear Reports produkt - bezpečnostná zraniteľnosť	Vysoká	**7.4**
12.	Red Hat Ansible Tower - bezpečnostná zraniteľnosť	Vysoká	**7.1**

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-362

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

Identifikátor

Siemens produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente spôsobiť pretečenie zásobníka a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2019-3823, CVE-2020-13987, CVE-2020-17437, CVE-2020-25236, CVE-2020-25239, CVE-2020-25240, CVE-2020-25241, CVE-2020-27632, CVE-2020-28385, CVE-2020-28387, CVE-2020-28388, CVE-2021-25667, CVE-2021-25673, CVE-2021-25674, CVE-2021-25675, CVE-2021-25676, CVE-2021-27380, CVE-2021-27381

Zasiahnuté systémy

RUGGEDCOM RM1224 vo verzii staršej ako v6.3 (vrátane)
SCALANCE M-800 vo verzii staršej ako v6.3 (vrátane)
SCALANCE S615 vo verzii staršej ako v6.3 (vrátane)
SCALANCE SC-600 vo verzii staršej ako v2.1.3
SCALANCE X300WG, Xx200 vo verzii staršej ako v4.1
SCALANCE XM400, XR500 vo verzii staršej ako v6.2
SIMATICS S7-PLCSIM v5.4 všetky verzie
SINEMA Remote Connect Server vo verzii staršej ako v3.0
LOGO! 8 BM všetky verzie
SENTRON 3VA COM100/800 všetky verzie
SENTRON 3VA DSP800 všetky verzie
SENTRON PAC2200 všetky verzie
SENTRON PAC3200 vo verzii staršej ako v2.4.7
SENTRON PAC3200T všetky verzie
SENTRON PAC3220 vo verzii staršej ako v3.2.0
SENTRON PAC4200 vo verzii staršej ako v2.3.0
SIMATIC MV400 vo verzii staršej ako v7.0.6
PLUSCONTROL 1st Gen všetky verzie
Solid Edge SE2020 vo verzii staršej ako SE2020MP13
Solid Edge SE2021 vo verzii staršej ako SE2021MP3

Následky

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

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://us-cert.cisa.gov/ics/advisories/icsa-21-068-03 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-03 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-01 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-04 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-05 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-06 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-07 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-08 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-09 https://us-cert.cisa.gov/ics/advisories/icsa-21-068-10 https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications

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

Identifikátor

Emerson Smart Wireless Gateway - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Emerson vydala bezpečnostné aktualizácie na produkt Smart Wireless Gateway, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorených HTTP požiadaviek vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2020-19417, CVE-2020-19419

Zasiahnuté systémy

Emerson Smart Wireless Gateway vo verzii staršej ako 1420 4.6.60

Následky

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

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/197940
https://exchange.xforce.ibmcloud.com/vulnerabilities/197939
https://packetstormsecurity.com/files/161700
https://seclists.org/fulldisclosure/2021/Mar/11

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Chrome, ktorá opravuje viacero kritických bezpečnostných zraniteľností.
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. Jedna zo zraniteľností je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

12.03.2021

CVE

CVE-2021-21191, CVE-2021-21192, CVE-2021-21193

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 89.0.4389.90

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 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://chromereleases.googleblog.com/2021/03/stable-channel-update-for-desktop_12.html
https://www.bleepingcomputer.com/news/security/google-fixes-second-actively-exploited-chrome-zero-day-this-month/
https://thehackernews.com/2021/03/another-google-chrome-0-day-bug-found.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/198135
https://exchange.xforce.ibmcloud.com/vulnerabilities/198136
https://exchange.xforce.ibmcloud.com/vulnerabilities/198137

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Madge - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Madge vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2021-23352

Zasiahnuté systémy

Madge vo verzii staršej ako 4.0.1

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

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.

Zdroje

https://snyk.io/vuln/SNYK-JS-MADGE-1082875
https://github.com/pahen/madge/commit/da5cbc9ab30372d687fa7c324b22af7ffa5c6332
https://www.npmjs.com/package/madge
https://exchange.xforce.ibmcloud.com/vulnerabilities/197915

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

Identifikátor

IBM DB2 - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na produkt DB2, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ďalšiu zraniteľnosť by vzdialený neautentifikovaný útočník mohol zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.03.2021

CVE

CVE-2020-5024, CVE-2020-5025

Zasiahnuté systémy

IBM Db2 vo verzii staršej ako V9.7 FP11
IBM Db2 vo verzii staršej ako V10.1 FP6
IBM Db2 vo verzii staršej ako V10.5 FP11
IBM Db2 vo verzii staršej ako V11.1 FP5
IBM Db2 vo verzii staršej ako V11.5.5

Následky

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

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/193660
https://exchange.xforce.ibmcloud.com/vulnerabilities/193661
https://www.ibm.com/support/pages/node/6427855

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TIBCO Spotfire - bezpečnostná zraniteľnosť

Popis

Spoločnosť TIBCO vydala bezpečnostnú aktualizáciu na produkt TIBCO Spotfire, ktorá opravuje bezpečnostnú zraniteľnosť.
Zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi získať neoprávnený prístup k autentifikačným údajom obete, následne eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2021-23273

Zasiahnuté systémy

TIBCO Spotfire Analyst vo verzii staršej ako 10.3.4
TIBCO Spotfire Analyst vo verzii staršej ako 10.10.3
TIBCO Spotfire Analyst vo verzii staršej ako 11.2.0
TIBCO Spotfire Analytics Platform pre AWS Marketplace vo verzii staršej ako 11.2.0
TIBCO Spotfire Server vo verzii staršej ako 10.3.12
TIBCO Spotfire Server vo verzii staršej ako 10.10.4
TIBCO Spotfire Server vo verzii staršej ako 11.2.0

Následky

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

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/197951
https://www.tibco.com/support/advisories/2021/03/tibco-security-advisory-march-9-2021-tibco-spotfire

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **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, autentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2021-21056, CVE-2021-21068, CVE-2021-21069, CVE-2021-21078, CVE-2021-21079, CVE-2021-21080, CVE-2021-21081, CVE-2021-21085

Zasiahnuté systémy

Adobe Framemaker vo verzii staršej ako 2020.0.2
Adobe Connect vo verzii staršej ako 11.2
Creative Cloud Desktop Application vo verzii staršej ako 5.4

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://helpx.adobe.com/security/products/framemaker/apsb21-14.html#Vulnerabilitydetails
https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-creative-cloud-adobe-connect-vulnerabilities/
https://threatpost.com/adobe-critical-flaws-windows/164611/
https://exchange.xforce.ibmcloud.com/vulnerabilities/197891
https://exchange.xforce.ibmcloud.com/vulnerabilities/197888
https://exchange.xforce.ibmcloud.com/vulnerabilities/197893
https://exchange.xforce.ibmcloud.com/vulnerabilities/197894
https://exchange.xforce.ibmcloud.com/vulnerabilities/197895

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

Identifikátor

Apache Oozie - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Oozie, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2020-35451

Zasiahnuté systémy

Apache Oozie vo verzii staršej ako 5.2.1

Následky

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

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/197899
https://seclists.org/oss-sec/2021/q1/200
https://oozie.apache.org/

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

Identifikátor

Schneider Electric IGSS SCADA - viacero zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na svoj produkt IGSS SCADA, ktorá opravuje 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

11.03.2021

CVE

CVE-2021-22709, CVE-2021-22710, CVE-2021-22711, CVE-2021-22712

Zasiahnuté systémy

IGSS Definition (Def.exe) vo verzii staršej ako 15.0.0.21042

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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-21-070-01

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

Identifikátor

Swagger Codegen - bezpečnostná zraniteľnosť

Popis

Spoločnosť Swagger vydala bezpečnostnú aktualizáciu na svoj produkt Codegen, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2021-21363

Zasiahnuté systémy

Swagger codegen vo verzii staršej ako 2.4.19

Následky

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

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/198072
https://github.com/swagger-api/swagger-codegen/security/advisories/GHSA-pc22-3g76-gm6j

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.4
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

I-net Clear Reports produkt - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu I-net Clear Reports.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného URL odkazu vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2020-28150

Zasiahnuté systémy

i-net Clear Reports vo verzii staršej ako 16.4 (vrátane)
i-net Clear Reports vo verzii staršej ako 19.2 (vrátane)
i-net Clear Reports vo verzii staršej ako 20.4 (vrátane)
i-net Clear Reports vo verzii staršej ako 20.10.136 (vrátane)

Následky

Neoprávnená zmena v systéme

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. 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.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/197952
https://c41nc.co.uk/cve-2020-28150/
https://www.inetsoftware.de/products/clear-reports

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

Identifikátor

Red Hat Ansible Tower - bezpečnostná zraniteľnosť

Popis

Spoločnosť Red Hat vydala bezpečnostnú aktualizáciu na svoj produkt Ansible Tower, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.03.2021

CVE

CVE-2021-20253

Zasiahnuté systémy

Red Hat Ansible Tower vo verzii staršej ako 3.8.2
Red Hat Ansible Tower vo verzii staršej ako 3.7.5
Red Hat Ansible Tower vo verzii staršej ako 3.6.7

Následky

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

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/197995
https://bugzilla.redhat.com/show_bug.cgi?id=1928847
https://access.redhat.com/security/cve/cve-2021-20253