BEZPEČNOSTNÝ BULLETIN

Týždeň 02. 02. 2022 - 08. 02. 2022

OBSAH BEZPEČNOSTNÉHO BULLETINU

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:
01794/2022/SK-CERT-676

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

Identifikátor

Foxit PDF Reader - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Foxit PDF Reader vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom povrhnutia špeciálne vytvoreného PDF súboru, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.01.2022

CVE

CVE-2021-40420

Zasiahnuté systémy

Foxit PDF Reader vo verzii staršej ako 11.1.0.52543

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1429
https://www.foxit.com/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40420
https://exchange.xforce.ibmcloud.com/vulnerabilities/218435

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:
01794/2022/SK-CERT-676

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

TensorFlow knižnica - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice TensorFlow vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.02.2022

CVE

CVE-2022-21728

Zasiahnuté systémy

TensorFlow vo verzii staršej ako 2.8.0

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
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://github.com/tensorflow/tensorflow/security/advisories/GHSA-6gmv-pjp9-p8w8
https://www.tensorflow.org/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21728
https://exchange.xforce.ibmcloud.com/vulnerabilities/218768

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Edge - bezpečnostná zraniteľnosť

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na produkt Edge, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.02.2022

CVE

CVE-2022-23263

Zasiahnuté systémy

Microsoft Edge vo verzii staršej ako 98.0.1108.43

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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2022-23263
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23263
https://exchange.xforce.ibmcloud.com/vulnerabilities/218722

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Argo CD - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja Argo CD vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorených paketov, získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

03.02.2022

CVE

CVE-2022-24348

Zasiahnuté systémy

Argo CD vo verzii staršej ako 2.3.0
Argo CD vo verzii staršej ako 2.2.4
Argo CD vo verzii staršej ako 2.1.9

Následky

Neoprávnený prístup k citlivým údajom

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://github.com/argoproj/argo-cd/security/advisories/GHSA-63qx-x74g-jcr7
https://packetstormsecurity.com/files/165850
https://apiiro.com/blog/malicious-kubernetes-helm-charts-can-be-used-to-steal-sensitive-information-from-argo-cd-deployments/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24348
https://exchange.xforce.ibmcloud.com/vulnerabilities/218803

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GitLab Community Edition a Enterprise Edition - viacero bezpečnostných zraniteľností

Popis

Vývojári nástroja GitLab vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky, získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

04.02.2022

CVE

CVE-2021-39931, CVE-2021-39943, CVE-2022-0123, CVE-2022-0136, CVE-2022-0167, CVE-2022-0249, CVE-2022-0283, CVE-2022-0344, CVE-2022-0371, CVE-2022-0373, CVE-2022-0390, CVE-2022-0425, CVE-2022-0427, CVE-2022-0477

Zasiahnuté systémy

GitLab Community Edition vo verzii staršej ako 14.7.1
GitLab Community Edition vo verzii staršej ako 14.6.4
GitLab Community Edition vo verzii staršej ako 14.5.4
GitLab Enterprise Edition vo verzii staršej ako 14.7.1
GitLab Enterprise Edition vo verzii staršej ako 14.6.4
GitLab Enterprise Edition vo verzii staršej ako 14.5.4

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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 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://about.gitlab.com/releases/2022/02/03/security-release-gitlab-14-7-1-released/
https://www.auscert.org.au/bulletins/ESB-2022.0501

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

Identifikátor

Apache ActiveMQ Artemis - bezpečnostná zraniteľnosť

Popis

Združenie Apache vydalo bezpečnostnú aktualizáciu na svoj produkt ActiveMQ Artemis, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky, spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.02.2022

CVE

CVE-2022-23913

Zasiahnuté systémy

Apache ActiveMQ Artemis vo verzii staršej ako 2.19.1
Apache ActiveMQ Artemis vo verzii staršej ako 2.20.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://seclists.org/oss-sec/2022/q1/122
https://activemq.apache.org/components/artemis/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23913
https://exchange.xforce.ibmcloud.com/vulnerabilities/218733