BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

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
Web: https://www.sk-cert.sk

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

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

Identifikátor

MS Azure HDInsight - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoj produkt Azure HDInsight, ktoré opravujú tri bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti nachádzajúce sa v komponentoch Apache Oozie Workflow Scheduler a Apache Ambari spočívajú v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorených požiadaviek eskalovať svoje privilégiá a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

6.2.2024

CVE

CVE-2023-36419, CVE-2023-38156

Zasiahnuté systémy

Azure HDInsight vo verzii staršej ako 2308221128

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

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://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36419
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38156

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

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

Identifikátor

Apple visionOS - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostnú aktualizáciu na operačný systém visionOS, ktorá opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2024-23222 sa nachádza v komponente WebKit a spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Spoločnosť Apple taktiež informovala, že daná bezpečnostná zraniteľnosť môže byť v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

31.1.2024

CVE

CVE-2024-23222

Zasiahnuté systémy

visionOS vo verzii staršej ako 1.0.2

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 získanie vzdialené vykonanie kódu, 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://support.apple.com/en-us/HT214070

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

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

Identifikátor

Red Hat JBoss Enterprise Application Platform - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Red Hat vydala bezpečnostnú aktualizáciu na svoj produkt Red Hat JBoss Enterprise Application Platform, ktorá opravuje 2 bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť s označením CVE-2023-4759 nachádzajúca sa v komponente jgit spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Bezpečnostnú zraniteľnosť s označením CVE-2023-44483 možno zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

7.2.2024

CVE

CVE-2023-44483, CVE-2023-4759

Zasiahnuté systémy

Red Hat JBoss Enterprise Application Platform vo verzii staršej ako 7.4.15

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
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 získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, 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://access.redhat.com/security/cve/CVE-2023-4759
https://access.redhat.com/security/cve/CVE-2023-44483

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

Identifikátor

Google Chrome - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Google Chrome, ktorá opravuje tri bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti nachádzajúce sa v komponentoch Skia a Mojo spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

6.2.2024

CVE

CVE-2024-1284, CVE-2024-1283

Zasiahnuté systémy

Google Chrome for Desktop – vo verzii staršej ako 121.0.6167.160/161 (Windows) a 121.0.6167.160 (Mac and Linux)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop.html

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

Identifikátor

Microsoft Edge - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Microsoft Edge, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sa nachádzajú v komponentoch Skia a Mojo, spočívaju v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

8.2.2024

CVE

CVE-2024-1283, CVE-2024-1284, CVE-2024-21399

Zasiahnuté systémy

Microsoft Edge Stable Channel vo verzii staršej ako 121.0.2277.113
Microsoft Edge Extended Stable Channel vo verzii staršej ako 120.0.2210.175

Následky

Zneprístupnenie služby
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.

Zdroje

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1283
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-1284
https://nvd.nist.gov/vuln/detail/CVE-2024-1284
https://nvd.nist.gov/vuln/detail/CVE-2024-1283

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

Identifikátor

Ivanti Connect Secure, Policy Secure a ZTA Gateways - bezpečnostná zraniteľnosť

Popis

Spoločnosť Ivanti vydala bezpečnostné aktualizácie na produkty Ivanti Connect Secure, Ivanti Policy Secure a ZTA, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2024-22024 nachádzajúca sa v komponente SAML spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k inak neprístupným zdrojom a získať tak neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

9.2.2024

CVE

CVE-2024-22024

Zasiahnuté systémy

Ivanti Connect Secure vo verziách starších ako 9.1R14.5, 9.1R17.3, 9.1R18.4, 22.4R2.3, 22.5R1.2, 22.5R2.3 a 22.6R2.2
Ivanti Policy Secure vo verziách starších ako 9.1R17.3, 9.1R18.4 a 22.5R1.2
ZTA Gateway vo verziiách starších ako 22.5R1.6, 22.6R1.5 a 22.6R1.7

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému
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://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

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

Identifikátor

VMware Aria Operations for Networks - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt VMware Aria Operations for Networks, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-22237 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a získať úplnú kontrolu nad systémom.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na vykonanie neoprávnených zmien v systéme, eskaláciu privilégií, získanie neoprávneného prístupu k citlivým údajom a na získanie neoprávneného prístupu do systému.

Dátum prvého zverejnenia varovania

6.2.2024

CVE

CVE-2024-22237, CVE-2024-22238, CVE-2024-22239, CVE-2024-22240, CVE-2024-22241

Zasiahnuté systémy

VMware Aria Operations for Networks vo verzii staršej ako 6.12.0

Následky

Vykonanie škodlivého kódu
Eskalácia privilégií
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://www.vmware.com/security/advisories/VMSA-2024-0002.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.6
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Lamassu Duoro zariadenia - 3 bezpečnostné zraniteľnosti

Popis

Spoločnosť Lammasu vydala bezpečnostnú aktualizáciu na svoje Bitcoinové bankomaty s označením Duoro, ktorá opravuje 3 bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu prostredníctvom podvrhnutia špeciálne vytvorených súborov získať úplnú kontrolu nad systémom.
Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkom.

Dátum prvého zverejnenia varovania

27.1.2024

CVE

CVE-2024-0175, CVE-2024-0176, CVE-2024-0177

IOC

Zasiahnuté systémy

Lamassu Duoro vo verzii staršej ako v8.1.5-1 a v8.1.6

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých zariadení. Ak je treba vykonať aktualizáciu systémov manuálne, postupujte podľa pokynov od výrobcu na webovej adrese uvedenej v sekcii ZDROJE.
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://support.lamassu.is/hc/en-us/articles/20747552619149-Security-update-for-Douros-2023-10-26- (manuálna aktualizácia zariadenia)
https://labs.ioactive.com/2024/01/atm-security-owning-bitcoin-atm.html
https://thehackernews.com/2024/01/allakore-rat-malware-targeting-mexican.html

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

Identifikátor

Cisco Secure Endpoint Connector/Private Cloud - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje produkty Secure Endpoint Connector for Windows a Secure Endpoint Private Cloud, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2024-20290 nachádzajúca sa v komponente ClamAV spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

7.2.2024

CVE

CVE-2024-20290

Zasiahnuté systémy

Cisco Secure Endpoint Connector for Windows vo verzii staršej ako 7.5.17 alebo vo verzii staršej ako 8.2.1
Cisco Secure Endpoint Private Cloud vo verzii staršej ako 3.8.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-hDffu6t

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

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

Identifikátor

Roundcube - bezpečnostná zraniteľnosť

Popis

Vývojári aplikácie Roundcube vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi, prostredníctvom cross-site scripting (XSS) útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

22.9.2023

CVE

CVE-2023-43770

Zasiahnuté systémy

Roundcube vo verzii staršej ako 1.4.14,
Roundcube 1.5.x vo verzii staršej ako 1.5.4
Roundcube 1.6.x vo verzii staršej ako 1.6.3

Následky

Získať neoprávnený prístup k citlivým údajom
Vykonať neoprávnené zmeny 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://github.com/roundcube/roundcubemail/releases/tag/1.6.3
https://lists.debian.org/debian-lts-announce/2023/09/msg00024.html
https://nvd.nist.gov/vuln/detail/CVE-2023-43770
https://www.cisa.gov/news-events/alerts/2024/02/12/cisa-adds-one-known-exploited-vulnerability-catalog

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
Web: https://www.sk-cert.sk

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

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

Identifikátor

Qolsys IQ Panel 4 a IQ4 Hub - bezpečnostná zraniteľnosť

Popis

Spoločnosť Qolsys vydala bezpečnostnú aktualizáciu na produkty IQ Panel 4 a IQ4 Hub, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2024-0242 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu získať neoprávnený prístup do systémových nastavení, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

8.2.2024

CVE

CVE-2024-0242

Zasiahnuté systémy

Qolsys IQ Panel 4 vo verzii staršej ako 4.4.2
Qolsys IQ4 Hub vo verzii staršej ako 4.4.2

Následky

Neoprávnený prístup do systému
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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2024/jci-psa-2024-03.pdf?la=en&hash=6962A644E2B944E1C667BB170EB54658BEB6A988
https://www.cisa.gov/news-events/ics-advisories/icsa-24-039-01

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
Web: https://www.sk-cert.sk

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

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

Identifikátor

AVEVA Edge - bezpečnostná zraniteľnosť

Popis

Spoločnosť AVEVA vydala bezpečnostnú aktualizáciu na svoj produkt AVEVA Edge (predtým známy ako InduSoft Web Studio), ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2023-6132 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného DLL súboru eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

1.2.2024

CVE

CVE-2023-6132

Zasiahnuté systémy

AVEVA Edge vo verzii staršej ako 2020 R2 SP2 (vrátane)

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://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/Security_Bulletin_AVEVA-2024-002.pdf
https://www.auscert.org.au/bulletins/ESB-2024.0727

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 02. 2024 - 13. 02. 2024

Dôležitosť	☐ **Nízka**	■ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.1
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

B&R Automation Runtime - bezpečnostná zraniteľnosť

Popis

Spoločnosť B&R vydala bezpečnostnú aktualizáciu na svoj produkt Automation Runtime, ktorá opravuje bezpečnostnú zrnaiteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2023-6028 nachádzajúca sa v komponente SDM (System Diagnostics Manager) spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý JavaScript kód a následne získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

5.2.2024

CVE

CVE-2023-6028

Zasiahnuté systémy

B&R Automation Runtime vo verzii staršej ako 14.93

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Pre dočasnú mitigáciu výrobca odporúča ponechávať System Diagnostics Manager deaktivovaný v čase, kedy ho nepoužívate.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.br-automation.com/fileadmin/SA23P018_SDM_Web_interface_vulnerable_to_XSS-1d75bee8.pdf

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
Web: https://www.sk-cert.sk