BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 02. 2024 - 27. 02. 2024

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
1.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	8.8
2.	Joomla! CMS - bezpečnostná zraniteľnosť	Vysoká	8.8
3.	IBM produkty - viacero bezpečnostných zraniteľností	Vysoká	8.8
4.	Mozilla produkty - viacero bezpečnostných zraniteľností	Vysoká	8.8
5.	GitLab - viacero bezpečnostných zraniteľností	Vysoká	8.7
6.	Atlassian produkty - viacero bezpečnostných zraniteľností	Vysoká	8.5
7.	B&R Automation Studio a Technology Guarding - bezpečnostná zraniteľnosť	Vysoká	8.3
8.	Linux Ubuntu - viacero bezpečnostných zraniteľností	Vysoká	8.0
9.	Delta Electronics CNCSoft-B DOPSoft - bezpečnostná zraniteľnosť	Vysoká	7.8
10.	PDF-XChange Editor - viacero bezpečnostných zraniteľností	Vysoká	7.5
11.	Open-source WiFi software (Android, ChromeOS, Linux) - dve bezpečnostné zraniteľnosti	Vysoká	7.5

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

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.8
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **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 bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-1669 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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

20.2.2024

CVE

CVE-2024-1669, CVE-2024-1670, CVE-2024-1671, CVE-2024-1672, CVE-2024-1673, CVE-2024-1674, CVE-2024-1675, CVE-2024-1676

Zasiahnuté systémy

Google Chrome vo verzii staršej ako 122.0.6261.57

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://chromereleases.googleblog.com/2024/02/stable-channel-update-for-desktop_20.html

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

Identifikátor

Joomla! CMS - bezpečnostná zraniteľnosť

Popis

Vývojári CMS Joomla! vydali bezpečnostnú aktualizáciu svojho produktu Joomla!, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Pre zneužitie zraniteľnosti sa vyžaduje interakcia používateľa s oprávnením administrátora, ktorý musí kliknúť na podvrhnutý škodlivý link.

Dátum prvého zverejnenia varovania

20.2.2024

CVE

CVE-2024-21726

Zasiahnuté systémy

Joomla! vo verzii staršej ako 3.10.15
Joomla! vo verzii staršej ako 4.4.3
Joomla! vo verzii staršej ako 5.0.3

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://developer.joomla.org/security-centre/929-20240205-core-inadequate-content-filtering-within-the-filter-code.html
https://www.thankyourobot.com/2024/02/joomla-releases-critical-update-to.html

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

Identifikátor

IBM produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2023-45133 sa nachádza v komponente traverse-7.20.13.tgz produktu IBM Maximo Application Suite, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom kompilácie špeciálne vytvoreného JavaScript kódu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby, vykonanie neoprávnených zmien v systéme a získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

19.2.2024

CVE

CVE-2023-35116, CVE-2023-39418, CVE-2023-5869, CVE-2023-22081, CVE-2023-22067, CVE-2023-5676, CVE-2023-45133, CVE-2023-45803, CVE-2023-50306, CVE-2023-43804, CVE-2023-25399, CVE-2023-29824, CVE-2023-29159, CVE-2023-27043, CVE-2023-44271

Zasiahnuté systémy

IBM Sterling Connect:Direct Web Services vo verzii staršej ako 6.3.0.6
IBM Sterling Connect:Direct Web Services vo verzii staršej ako 6.2.0.22
IBM Sterling Connect:Direct Web Services vo verzii staršej ako 6.1.0.23
IBM Sterling Connect:Direct Web Services vo všetkých verziách 6.0.x
IBM Maximo Application Suite vo verzii staršej ako 8.11.6
IBM Maximo Application Suite vo verzii staršej ako 8.10.9
IBM Truststore Manager vo verzii staršej ako 8.10.9
IBM Truststore Manager vo verzii staršej ako 8.11.6 (CVE-2023-45803 a CVE-2023-43804)
IBM Truststore Manager vo verzii staršej ako 8.11.5 (CVE-2023-45133)
IBM Common Licensing vo verzii staršej ako (vrátane) Agent 9.0
IBM Business Automation Workflow containers vo verzii staršej ako 23.0.2-IF001
IBM Business Automation Workflow traditional vo verzii staršej ako 23.0.2-IF001

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnená zmena v systéme
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 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://www.ibm.com/support/pages/node/7120595
https://www.ibm.com/support/pages/node/7120672
https://www.ibm.com/support/pages/node/7120589

https://www.ibm.com/support/pages/node/7120591
https://www.ibm.com/support/pages/node/7120592
https://www.ibm.com/support/pages/node/7120658
https://www.ibm.com/support/pages/node/7120660
https://www.ibm.com/support/pages/node/7120748

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

Identifikátor

Mozilla produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na svoje produkty Firefox, Firefox ESR a Thunderbird, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s označeniami CVE-2024-1557 a CVE-2024-1553 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. Zneužitie zraniteľností vyžaduje interakciu zo strany používateľov.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.2.2024

CVE

CVE-2024-1546, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1551, CVE-2024-1552, CVE-2024-1553, CVE-2024-1554, CVE-2024-1555, CVE-2024-1556, CVE-2024-1557

Zasiahnuté systémy

Firefox vo verzii staršej ako 123
Firefox ESR vo verzii staršej ako 115.8
Thunderbird vo verzii staršej ako 115.8

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 vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialné 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2024-07/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-06/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-05/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.7
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GitLab - viacero bezpečnostných zraniteľností

Popis

Vývojári platformy GitLab vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-1451 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Pre zneužitie zraniteľnosti sa vyžaduje interakcia používateľa.
Ostatné bezpečnotné zraniteľnosti môžu útočníkom umožniť získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

21.2.2024

CVE

CVE-2024-1451, CVE-2023-6477, CVE-2023-6736, CVE-2024-1525, CVE-2023-4895, CVE-2024-0861, CVE-2023-3509, CVE-2024-0410

Zasiahnuté systémy

GitLab Community Edition (CE) vo verzii staršej ako 16.9.1, 16.8.3 a 16.7.6
GitLab Enterprise Edition (EE) vo verzii staršej ako 16.9.1, 16.8.3 a 16.7.6

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://about.gitlab.com/releases/2024/02/21/security-release-gitlab-16-9-1-released/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Atlassian produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Atlassian vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-21678 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v produkte Confluence Data Center and Server a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom stored cross-site scripting (stored XSS) útoku vykonať škodlivý kód s následkom narušenia dôvernosti a integrity systému.
Ostatné bezpečnotné zraniteľnosti môžu útočníkom umožniť získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.2.2024

CVE

CVE-2024-21678, CVE-2023-5072, CVE-2023-6481, CVE-2023-6378, CVE-2023-46589, CVE-2023-39410, CVE-2023-41835, CVE-2023-2976, CVE-2023-46589, CVE-2024-21682, CVE-2023-2976

Zasiahnuté systémy

Confluence Data Center and Server
Jira Software Data Center and Server
Assets Discovery
Jira Service Management Data Center and Server

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Vykonanie škodlivého kódu a narušenie dôvernosti a integrity systému
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 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://confluence.atlassian.com/security/security-bulletin-february-20-2024-1354501606.html
https://jira.atlassian.com/browse/CONFSERVER-94513

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

Identifikátor

B&R Automation Studio a Technology Guarding - bezpečnostná zraniteľnosť

Popis

Spoločnosť B&R vydala bezpečnostné aktualizácie na svoje produkty Automation Studio a Technology Guarding, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2024-0220 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.2.2024

CVE

CVE-2024-0220

Zasiahnuté systémy

B&R Automation Studio vo verzii staršej ako 4.6
B&R Technology Guarding vo verzii staršej ako 1.4.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu uvedených na odkaze v sekcii ZDROJE.
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.
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.br-automation.com/fileadmin/SA23P019_Automation_Studio_Upgrade_Service_uses_insufficient_encryption.pdf-1b3b181c.pdf

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

Identifikátor

Linux Ubuntu - viacero bezpečnostných zraniteľností

Popis

Vývojári distribúcie Ubuntu open source operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0985 nachádzajúca sa v komponente postgresql-12, 14 a 15 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby, neoprávnený prístup k citlivým údajom a neoprávnenú zmenu v systéme.

Dátum prvého zverejnenia varovania

26.2.2024

CVE

CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952, CVE-2024-20932, CVE-2022-43244, CVE-2022-43249, CVE-2022-43250, CVE-2022-47665, CVE-2023-25221, CVE-2022-43245, CVE-2023-24751, CVE-2023-24752, CVE-2023-24754, CVE-2023-24755, CVE-2023-24756, CVE-2023-24757, CVE-2023-24758, CVE-2024-25062, CVE-2023-50387, CVE-2023-50868, CVE-2023-28450, CVE-2024-0985, CVE-2022-47695, CVE-2022-48063, CVE-2022-48065, CVE-2023-43770

Zasiahnuté systémy

Ubuntu 23.10:
postgresql-15 vo verzii staršej ako 15.6-0ubuntu0.23.10.1
postgresql-client-15 vo verzii staršej ako 15.6-0ubuntu0.23.10.1
openjdk-11-jdk vo verzii staršej ako 11.0.22+7-0ubuntu2~23.10.1
openjdk-11-jdk-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~23.10.1
openjdk-11-jre vo verzii staršej ako 11.0.22+7-0ubuntu2~23.10.1
openjdk-11-jre-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~23.10.1
openjdk-11-jre-zero vo verzii staršej ako 11.0.22+7-0ubuntu2~23.10.1
openjdk-21-jdk vo verzii staršej ako 21.0.2+13-1~23.10.1
openjdk-21-jdk-headless vo verzii staršej ako 21.0.2+13-1~23.10.1
openjdk-21-jre vo verzii staršej ako 21.0.2+13-1~23.10.1
openjdk-21-jre-headless vo verzii staršej ako 21.0.2+13-1~23.10.1
openjdk-21-jre-zero vo verzii staršej ako 21.0.2+13-1~23.10.1
openjdk-17-jdk vo verzii staršej ako 17.0.10+7-1~23.10.1
openjdk-17-jdk-headless vo verzii staršej ako 17.0.10+7-1~23.10.1
openjdk-17-jre vo verzii staršej ako 17.0.10+7-1~23.10.1
openjdk-17-jre-headless vo verzii staršej ako 17.0.10+7-1~23.10.1
openjdk-17-jre-zero vo verzii staršej ako 17.0.10+7-1~23.10.1
libxml2 vo verzii staršej ako 2.9.14+dfsg-1.3ubuntu0.1
dnsmasq-base vo verzii staršej ako 2.90-0ubuntu0.23.10.1
roundcube vo verzii staršej ako 1.6.2+dfsg-1ubuntu0.1
roundcube-core vo verzii staršej ako 1.6.2+dfsg-1ubuntu0.1

Ubuntu 22.04:
postgresql-14 vo verzii staršej ako 14.11-0ubuntu0.22.04.1
postgresql-client-14 vo verzii staršej ako14.11-0ubuntu0.22.04.1
openjdk-11-jdk vo verzii staršej ako 11.0.22+7-0ubuntu2~22.04.1

openjdk-11-jdk-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~22.04.1
openjdk-11-jre vo verzii staršej ako 11.0.22+7-0ubuntu2~22.04.1
openjdk-11-jre-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~22.04.1
openjdk-11-jre-zero vo verzii staršej ako 11.0.22+7-0ubuntu2~22.04.1
openjdk-21-jdk vo verzii staršej ako 21.0.2+13-1~22.04.1
openjdk-21-jdk-headless vo verzii staršej ako 21.0.2+13-1~22.04.1
openjdk-21-jre vo verzii staršej ako 21.0.2+13-1~22.04.1
openjdk-21-jre-headless vo verzii staršej ako 21.0.2+13-1~22.04.1
openjdk-21-jre-zero vo verzii staršej ako 21.0.2+13-1~22.04.1
openjdk-17-jdk vo verzii staršej ako 17.0.10+7-1~22.04.1
openjdk-17-jdk-headless vo verzii staršej ako 17.0.10+7-1~22.04.1
openjdk-17-jre vo verzii staršej ako 17.0.10+7-1~22.04.1
openjdk-17-jre-headless vo verzii staršej ako 17.0.10+7-1~22.04.1
openjdk-17-jre-zero vo verzii staršej ako 17.0.10+7-1~22.04.1
libde265-0 vo verzii staršej ako 1.0.8-1ubuntu0.2
libxml2 vo verzii staršej ako 2.9.13+dfsg-1ubuntu0.4
dnsmasq-base vo verzii staršej ako 2.90-0ubuntu0.22.04.1
binutils vo verzii staršej ako 2.38-4ubuntu2.6
binutils-multiarch vo verzii staršej ako 2.38-4ubuntu2.6
roundcube vo verzii staršej ako 1.5.0+dfsg.1-2ubuntu0.1~esm2
roundcube-core vo verzii staršej ako 1.5.0+dfsg.1-2ubuntu0.1~esm2

Ubuntu 20.04:
postgresql-12 vo verzii staršej ako 12.18-0ubuntu0.20.04.1
postgresql-client-12 vo verzii staršej ako 12.18-0ubuntu0.20.04.1
openjdk-11-jdk vo verzii staršej ako 11.0.22+7-0ubuntu2~20.04.1
openjdk-11-jdk-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~20.04.1
openjdk-11-jre vo verzii staršej ako 11.0.22+7-0ubuntu2~20.04.1
openjdk-11-jre-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~20.04.1
openjdk-11-jre-zero vo verzii staršej ako 11.0.22+7-0ubuntu2~20.04.1
openjdk-21-jdk vo verzii staršej ako 21.0.2+13-1~20.04.1
openjdk-21-jdk-headless vo verzii staršej ako 21.0.2+13-1~20.04.1
openjdk-21-jre vo verzii staršej ako 21.0.2+13-1~20.04.1
openjdk-21-jre-headless vo verzii staršej ako 21.0.2+13-1~20.04.1
openjdk-21-jre-zero vo verzii staršej ako 21.0.2+13-1~20.04.1
openjdk-17-jdk vo verzii staršej ako 17.0.10+7-1~20.04.1
openjdk-17-jdk-headless vo verzii staršej ako 17.0.10+7-1~20.04.1
openjdk-17-jre vo verzii staršej ako 17.0.10+7-1~20.04.1
openjdk-17-jre-headless vo verzii staršej ako 17.0.10+7-1~20.04.1
openjdk-17-jre-zero vo verzii staršej ako 17.0.10+7-1~20.04.1
libde265-0 vo verzii staršej ako 1.0.4-1ubuntu0.3
libxml2 vo verzii staršej ako 2.9.10+dfsg-5ubuntu0.20.04.7
dnsmasq-base vo verzii staršej ako 2.90-0ubuntu0.20.04.1
binutils vo verzii staršej ako 2.34-6ubuntu1.9
binutils-multiarch vo verzii staršej ako 2.34-6ubuntu1.9
roundcube vo verzii staršej ako 1.4.3+dfsg.1-1ubuntu0.1~esm3
roundcube-core vo verzii staršej ako 1.4.3+dfsg.1-1ubuntu0.1~esm3

Ubuntu 18.04:
openjdk-11-jdk vo verzii staršej ako 11.0.22+7-0ubuntu2~18.04.1
openjdk-11-jdk-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~18.04.1
openjdk-11-jre vo verzii staršej ako 11.0.22+7-0ubuntu2~18.04.1
openjdk-11-jre-headless vo verzii staršej ako 11.0.22+7-0ubuntu2~18.04.1
openjdk-11-jre-zero vo verzii staršej ako 11.0.22+7-0ubuntu2~18.04.1
openjdk-17-jdk vo verzii staršej ako 17.0.10+7-1~18.04.1
openjdk-17-jdk-headless vo verzii staršej ako 17.0.10+7-1~18.04.1
openjdk-17-jre vo verzii staršej ako 17.0.10+7-1~18.04.1
openjdk-17-jre-headless vo verzii staršej ako 17.0.10+7-1~18.04.1
openjdk-17-jre-zero vo verzii staršej ako 17.0.10+7-1~18.04.1
libde265-0 vo verzii staršej ako 1.0.2-2ubuntu0.18.04.1~esm3
roundcube vo verzii staršej ako 1.3.6+dfsg.1-1ubuntu0.1~esm3
roundcube-core vo verzii staršej ako 1.3.6+dfsg.1-1ubuntu0.1~esm3

Ubuntu 16.04:
libde265-0 vo verzii staršej ako 1.0.2-2ubuntu0.16.04.1~esm3
roundcube vo verzii staršej ako 1.2~beta+dfsg.1-0ubuntu1+esm3
roundcube-core vo verzii staršej ako 1.2~beta+dfsg.1-0ubuntu1+esm3

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 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://ubuntu.com/security/CVE-2024-0985
https://ubuntu.com/security/notices/USN-6662-1
https://ubuntu.com/security/notices/USN-6661-1
https://ubuntu.com/security/notices/USN-6659-1
https://ubuntu.com/security/notices/USN-6658-1
https://ubuntu.com/security/notices/USN-6657-1
https://ubuntu.com/security/notices/USN-6656-1
https://ubuntu.com/security/notices/USN-6655-1
https://ubuntu.com/security/notices/USN-6654-1
https://ubuntu.com/security/notices/USN-6660-1

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

Identifikátor

Delta Electronics CNCSoft-B DOPSoft - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft-B DOPSoft, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2024-1595 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného DLL súboru vykonať škodlivý kód a získať úplnú kontrolu nad systémom. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

22.2.2024

CVE

CVE-2024-1595

Zasiahnuté systémy

CNCSoft-B v1.0.0.4 DOPSoft vo verzii staršej ako v4.0.0.94

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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.
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.cisa.gov/news-events/ics-advisories/icsa-24-053-01

BEZPEČNOSTNÝ BULLETIN

Týždeň 21. 02. 2024 - 27. 02. 2024

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

Identifikátor

PDF-XChange Editor - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Tracker Software vydala bezpečnostnú aktualizáciu na produkty PDF-XChange Editor, PDF-Tools a PDF-XChange PRO, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2024-27327 a CVE-2024-27323 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

23.2.2024

CVE

CVE-2024-27327, CVE-2024-27326, CVE-2024-27325, CVE-2024-27328, CVE-2024-27331, CVE-2024-27329, CVE-2024-27330, CVE-2024-27332, CVE-2024-27323, CVE-2024-27324

Zasiahnuté systémy

PDF-XChange Editor vo verzii staršej ako 10.1.3.383
PDF-Tools vo verzii staršej ako 10.1.3.383
PDF-XChange PRO vo verzii staršej ako 10.1.3.383

Následky

Vykonanie škodlivého kódu a 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 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://www.pdf-xchange.com/support/security-bulletins.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/283976
https://exchange.xforce.ibmcloud.com/vulnerabilities/283968
https://exchange.xforce.ibmcloud.com/vulnerabilities/283974
https://exchange.xforce.ibmcloud.com/vulnerabilities/283973
https://exchange.xforce.ibmcloud.com/vulnerabilities/283972
https://exchange.xforce.ibmcloud.com/vulnerabilities/283971
https://exchange.xforce.ibmcloud.com/vulnerabilities/283970
https://exchange.xforce.ibmcloud.com/vulnerabilities/283969
https://exchange.xforce.ibmcloud.com/vulnerabilities/283967
https://exchange.xforce.ibmcloud.com/vulnerabilities/283975

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 21. 02. 2024 - 27. 02. 2024

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

Identifikátor

Open-source WiFi software (Android, ChromeOS, Linux) - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach v open-source WiFi softvéri pre operačné systémy Android, Linux a ChromeOS.

Bezpečnostná zraniteľnosť s označením CVE-2023-52160 sa nachádza v komponente wpa_supplicant. spočíva v nedostatočnej implementácii bezpečnostných mechanizmov, umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vytvoriť klon dôveryhodnej WiFi siete a následne prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom. Zraniteľné sú len WiFi siete používajúce režim WPA2/3 Enterprise.

Bezpečnostná zraniteľnosť s označením CVE-2023-52161 sa nachádza v komponente Intel's iNet Wireless Daemon (IWD), spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne upravených príkazov získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

13.2.2024

CVE

CVE-2023-52160, CVE-2023-52161

Zasiahnuté systémy

wpa_supplicant vo verzii staršej ako v2.10 (vrátane)
IWD vo verzii staršej ako 2.14
ChromeOS vo verzii staršej ako 118
Android vo všetkých verziách
Linux vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Pre operačné systémy Android, prípadne iné nepodporované systémy, je odporúčaná manuálna konfigurácia certifikátu CA pre všetky uložené podnikové siete. Taktiež sa odporúča zrušiť všetky nepoužívané siete WPA2/3 Enterprise a vypnúť automatické pripojenie do sietí tohto typu. Detailné inštrukcie môžete nájsť na webovej adrese:
https://www.top10vpn.com/research/wifi-vulnerabilities/

Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.

Zdroje

https://www.top10vpn.com/research/wifi-vulnerabilities/
https://thehackernews.com/2024/02/new-wi-fi-vulnerabilities-expose.html
https://access.redhat.com/security/cve/cve-2023-52160
https://www.suse.com/security/cve/CVE-2023-52161.html
https://security-tracker.debian.org/tracker/CVE-2023-52161

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