BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 02. 2024 - 05. 03. 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

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

Identifikátor

WordPress Slider Responsive Slideshow - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu Slider Responsive Slideshow – Image slider, Gallery slideshow vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1859 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injektovania špeciálne vytvoreného PHP kódu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Ak je v zasiahnutom systéme prítomný POP chain, napríklad prostredníctvom iného nainštalovaného pluginu, možno predmetnú zraniteľnosť zneužiť na odstránenie ľubovoľných súborov v zasiahnutom systéme, neoprávnený prístup k citlivým údajom a vzdialené vykonanie kódu.

Dátum prvého zverejnenia varovania

29.3.2024

CVE

CVE-2024-1859

Zasiahnuté systémy

Slider Responsive Slideshow – Image slider, Gallery slideshow vo verzii staršej ako 1.4.0

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/slider-responsive-slideshow/slider-responsive-slideshow-image-slider-gallery-slideshow-138-authenticated-contributor-php-object-injection

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

Identifikátor

WordPress Conversios plugin - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o dvoch kritických bezpečnostných zraniteľnostiach WordPress pluginu Conversios.
Kritické bezpečnostné zraniteľnosti s identifikátormi CVE-2024-0786 a CVE-2024-1203 spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Predmetný plugin už nie je naďalej udržiavaný.

Dátum prvého zverejnenia varovania

28.3.2024

CVE

CVE-2024-0786, CVE-2024-1203

Zasiahnuté systémy

WordPress Conversios plugin vo všetkých verziách

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin. V prípade, že áno, odporúčame prejsť na iný produkt s platnou podporou (produkt už nie je udržiavaný).
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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/enhanced-e-commerce-for-woocommerce-store/conversios-691-authenticated-subscriber-sql-injection-via-ee-syncproductcategory
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/enhanced-e-commerce-for-woocommerce-store/conversios-google-analytics-4-ga4-meta-pixel-more-via-google-tag-manager-for-woocommerce-691-authenticated-subscriber-sql-injection

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

Identifikátor

Chrome - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Chrome, ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti 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 bezpečnostných zraniteľností vyžaduje interakciu používateľa. Zraniteľnosti aktuálne nemajú pridelené identifikátory CVE.

Dátum prvého zverejnenia varovania

27.2.2024

CVE

CVE-2024-1938, CVE-2024-1939

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 122.0.6261.94
Chrome pre Windows vo verzii staršej ako 122.0.6261.94/.95 (bezpečnostná záplata pre Windows bude sprístupnená v nasledujúcich dňoch/týždňoch)

Následky

Vykonanie škodlivého kódu
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.
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_27.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/284232
https://exchange.xforce.ibmcloud.com/vulnerabilities/284231

BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 02. 2024 - 05. 03. 2024

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

Identifikátor

Red Hat produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Red Hat vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Závažná bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25617 sa nachádza v komponente squid produktu Red Hat Enterprise Linux, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej HTTP požiadavky spôsobiť zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

4.3.2024

CVE

CVE-2024-25617, CVE-2023-45234, CVE-2023-45230, CVE-2023-50269, CVE-2007-4559, CVE-2020-10735, CVE-2020-17049, CVE-2020-24736, CVE-2020-28241, CVE-2021-35937, CVE-2021-35938, CVE-2021-35939, CVE-2021-46848, CVE-2022-35252, CVE-2022-35737, CVE-2022-36227, CVE-2022-37434, CVE-2022-40303, CVE-2022-40304, CVE-2022-40897, CVE-2022-43552, CVE-2022-43680, CVE-2022-45061, CVE-2022-48468, CVE-2022-48560, CVE-2022-48564, CVE-2023-1667, CVE-2023-2283, CVE-2023-2602, CVE-2023-2603, CVE-2023-3446, CVE-2023-3817, CVE-2023-4641, CVE-2023-4806, CVE-2023-4813, CVE-2023-5455, CVE-2023-5678, CVE-2023-5981, CVE-2023-27043, CVE-2023-27535, CVE-2023-27536, CVE-2023-28322, CVE-2023-28484, CVE-2023-29469, CVE-2023-29491, CVE-2023-32681, CVE-2023-39326, CVE-2023-39615, CVE-2023-43804, CVE-2023-45287, CVE-2023-45803, CVE-2023-46218, CVE-2023-48795, CVE-2022-45939, CVE-2022-48337, CVE-2022-48339, CVE-2022-3287

Zasiahnuté systémy

squid vo verzii staršej ako 6.5
Red Hat CodeReady Linux Builder
Red Hat Enterprise Linux
Red Hat Enterprise Linux Server

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
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.
Pre dočasnú mitigáciu bezpečnostnej zraniteľnosti v komponente squid odporúčame postupovať podľa pokynov výrobcu uvedených na webovej adrese: https://access.redhat.com/security/cve/CVE-2024-25617
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://access.redhat.com/errata/RHSA-2024:1066
https://github.com/squid-cache/squid/security/advisories/GHSA-h5x6-w8mv-xfpr

https://access.redhat.com/security/cve/CVE-2024-25617
https://access.redhat.com/errata/RHSA-2024:1063
https://access.redhat.com/security/cve/CVE-2023-45230
https://access.redhat.com/security/cve/CVE-2023-45234
https://access.redhat.com/errata/RHSA-2024:1108
https://access.redhat.com/errata/RHSA-2024:1110
https://access.redhat.com/errata/RHSA-2024:1112
https://access.redhat.com/errata/RHSA-2024:1113

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

Identifikátor

Kofax Power PDF - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Kofax vydala bezpečnostné aktualizácie na svoj produkt Power PDF, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

19.2.2024

CVE

Zasiahnuté systémy

Kofax Power PDF Advanced vo verzii staršej ako 5.0.0.18

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 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://docshield.tungstenautomation.com/PowerPDF/en_US/5.0.0-3uoz7ssq2b/print/ReadMe-KofaxPowerPDFAdvanced-5.0.0.18.htm
https://www.zerodayinitiative.com/advisories/ZDI-24-216/
https://www.zerodayinitiative.com/advisories/ZDI-24-217/
https://www.zerodayinitiative.com/advisories/ZDI-24-218/
https://www.zerodayinitiative.com/advisories/ZDI-24-219/
https://www.zerodayinitiative.com/advisories/ZDI-24-220/
https://www.zerodayinitiative.com/advisories/ZDI-24-221/
https://www.zerodayinitiative.com/advisories/ZDI-24-222/
https://www.zerodayinitiative.com/advisories/ZDI-24-223/
https://www.zerodayinitiative.com/advisories/ZDI-24-224/
https://www.zerodayinitiative.com/advisories/ZDI-24-225/
https://www.zerodayinitiative.com/advisories/ZDI-24-226/
https://www.zerodayinitiative.com/advisories/ZDI-24-227/
https://www.zerodayinitiative.com/advisories/ZDI-24-228/
https://www.zerodayinitiative.com/advisories/ZDI-24-229/
https://www.zerodayinitiative.com/advisories/ZDI-24-230/
https://www.zerodayinitiative.com/advisories/ZDI-24-231/
https://www.zerodayinitiative.com/advisories/ZDI-24-232/

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

WordPress Avada theme - dve bezpečnostné zraniteľnosti

Popis

Vývojári WordPress pluginu Avada vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-1468 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvoreného súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.2.2024

CVE

CVE-2024-1668, CVE-2024-1468

Zasiahnuté systémy

WordPress Avada theme vo verzii staršej ako 7.11.5

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.wordfence.com/threat-intel/vulnerabilities/wordpress-themes/Avada/avada-website-builder-for-wordpress-woocommerce-7114-authenticated-contributor-arbitrary-file-upload

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

Identifikátor

WordPress Vimeography - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti WordPress pluginu Vimeography.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0825 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie PHP objektu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ak je v zasiahnutom systéme prítomný POP chain, napríklad prostredníctvom iného nainštalovaného pluginu, možno predmetnú zraniteľnosť zneužiť na odstránenie ľubovoľných súborov v zasiahnutom systéme, neoprávnený prístup k citlivým údajom a vzdialené vykonanie kódu.

Dátum prvého zverejnenia varovania

4.3.2024

CVE

Zasiahnuté systémy

WordPress plugin Vimeography vo všetkých verziách

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii.
V prípade, že áno, odporúčame zvážiť prechod na plugin s platnou podporou, prípadne zvážiť jeho úplné odstránenie.
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://wordpress.org/plugins/vimeography/#description
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/vimeography/vimeography-vimeo-video-gallery-wordpress-plugin-232-authenticated-contributor-php-object-injection

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

Identifikátor

WordPress Auto Refresh Single Page plugin - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti WordPress pluginu Auto Refresh Single Page. Bezpečnostná zraniteľnosť s označením CVE-2024-1731 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injektovania špeciálne vytvoreného PHP kódu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Ak je v zasiahnutom systéme prítomný POP chain, napríklad prostredníctvom iného nainštalovaného pluginu, možno predmetnú zraniteľnosť zneužiť na odstránenie ľubovoľných súborov v zasiahnutom systéme, neoprávnený prístup k citlivým údajom a vzdialené vykonanie kódu.
Predmetný plugin už nie je naďalej udržiavaný.

Dátum prvého zverejnenia varovania

4.3.2024

CVE

CVE-2024-1731

Zasiahnuté systémy

Auto Refresh Single Page plugin vo všetkých verziách

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin. V prípade, že áno, odporúčame prejsť na iný produkt s platnou podporou (produkt už nie je udržiavaný).
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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/auto-refresh-single-page/auto-refresh-single-page-11-authenticated-contributor-php-object-injection

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

Identifikátor

Cisco produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-20321 sa nachádza v komponente External Border Gateway Protocol (eBGP) operačného systému Cisco NX-OS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zahltenia sieťovej prevádzky spôsobiť zneprístupnenie služby.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-20267 sa nachádza v komponente MPLS traffic operačného systému Cisco NX-OS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania IPv6 špeciálne upravených paketov spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti môžu spôsobiť zneprístupnenie služby alebo vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

28.2.2024

CVE

CVE-2024-20321, CVE-2024-20267, CVE-2024-20344, CVE-2024-20291, CVE-2024-20294

Zasiahnuté systémy

Cisco NX-OS na Cisco Nexus 3600 Series Switches (Cisco ID: N3K-C36180YC-R, N3K-C3636C-R, N9K-X9624D-R2, N9K-X9636C-R, N9K-X9636C-RX, N9K-X9636Q-R, N9K-X96136YC-R)
Cisco NX-OS na Cisco Nexus 9500 R-Series Line Cards (Cisco ID: N3K-C36180YC-R, N3K-C3636C-R, N9K-X9624D-R2, N9K-X9636C-R, N9K-X9636C-RX, N9K-X9636Q-R, N9K-X96136YC-R)
Cisco NX-OS na Nexus 3000 Series Switches
Cisco NX-OS na Nexus 5500 Platform Switches
Cisco NX-OS na Nexus 5600 Platform Switches
Cisco NX-OS na Nexus 6000 Series Switches
Cisco NX-OS na Nexus 7000 Series Switches
Cisco NX-OS na Nexus 9000 Series Switches
Cisco UCS 6400
Cisco UCS 6500

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

Zneprístupnenie služby
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsfi-imm-syn-p6kZTDQC
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-po-acl-TkyePgvL
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-lldp-dos-z7PncTgt

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:** 8.6
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco NX-OS - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na svoje portfólio produktov prevádzkujúce NX-OS softvér, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti s identifikátormi CVE-2024-20267 a CVE-2024-20321 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného IPv6 paketu alebo
zaslaním veľkého množstva sieťovej prevádzky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.2.2024

CVE

CVE-2024-20267, CVE-2024-20321

Zasiahnuté systémy

Cisco NX-OS Software vo verzii 9.3(12) prevádzkovaný na platformách Nexus 3000 a 9000 Series Switches bez nainštalovanej aktualizácie nxos.CSCwh42690-n9k_ALL-1.0.0-9.3.12.lib32_n9000.rpm
Cisco NX-OS Software vo verzii 9.3(12) prevádzkovaný na platformách Nexus 3600 Switches a Nexus 9500 R-Series Line Cards bez nainštalovanej aktualizácie nxos.CSCwh09703-n9k_ALL-1.0.0-9.3.12.lib32_n9000.rpm
Cisco NX-OS Software vo verzii 10.2(6) prevádzkovaný na platformách Nexus 3000 a 9000 Series Switches bez nainštalovanej aktualizácie nxos64-cs.CSCwh42690-1.0.0-10.2.6.lib32_64_n9000.rpm alebo nxos64-msll.CSCwh42690-1.0.0-10.2.6.lib32_64_n9000.rpm
Cisco NX-OS Software vo verzii 10.2(6) prevádzkovaný na platformách Nexus 3600 Switches a Nexus 9500 R-Series Line Cards bez nainštalovanej aktualizácie nxos64-msll.CSCwh09703-1.0.0-10.2.6.lib32_64_n9000.rpm
Cisco NX-OS Software vo verzii 10.3(4a) prevádzkovaný na platforme Nexus 9500 R-Series Line Cards bez nainštalovanej aktualizácie nxos64-msll.CSCwh96478-1.0.0-10.3.4a.lib32_64_n9000.rpm

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM

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

Identifikátor

Mitel Networks MiContact Center Business - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Mitel Networks vydala bezpečnostnú aktualizáciu na svoj produkt MiContact Center Business, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia 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.
Zraniteľnostiam nebol pridelený identifikátor CVE.

Dátum prvého zverejnenia varovania

29.2.2024

CVE

Zasiahnuté systémy

MiContact Center Business vo verzii staršej ako 9.4.2.0, 9.5.0.3 a 10.0.0.4 (vrátane) bez aplikovanej bezpečnostnej záplaty

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov, a na aktualizované verzie aplikovať bezpečnostnú záplatu. Odkaz na stiahnutie pre zákazníkov sa nachádza na webových adresách uvedených 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.
Výrobca odporúča na aktualizované verzie aplikovať bezpečnostnú záplatu. Odkaz na stiahnutie pre zákazníkov sa nachádza na webových adresách uvedených v sekcii ZDROJE.

Zdroje

https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin_24-0001-001-v1.pdf
https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin_24-0002-001-v1.pdf

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

Identifikátor

WordPress LiteSpeed Plugin - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu LiteSpeed vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť s identifikátorom CVE-2023-40000 sa nachádza vo voliteľnom plugine LiteSpeed pre WordPress, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom stored cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

25.10.2023

CVE

CVE-2023-40000

Zasiahnuté systémy

LiteSpeed Cache vo verzii staršej ako 5.7.0.1

Následky

Vykonanie škodlivého kódu
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://patchstack.com/database/vulnerability/litespeed-cache/wordpress-litespeed-cache-plugin-5-7-unauthenticated-site-wide-stored-xss-vulnerability
https://patchstack.com/articles/xss-vulnerability-in-litespeed-cache-plugin-affecting-4-million-sites/
https://securityonline.info/cve-2023-40000-xss-alert-patch-litespeed-cache-plugin-immediately/?expand_article=1

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Microsoft Edge - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Microsoft vydala bezpečnostnú aktualizáciu na svoj prehliadač Microsoft Edge, ktorá opravuje 3 bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-26192 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby.
Jej zneužitie tiež umožňuje únik zo sandboxu a následné ďalšie útoky proti systému.

Dátum prvého zverejnenia varovania

23.2.2024

CVE

CVE-2024-26192, CVE-2024-26188, CVE-2024-21423

Zasiahnuté systémy

Microsoft Edge (Chromium-based) vo verzii staršej ako 122.0.2365.52

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

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.
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-2024-26188
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21423
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26192

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

Identifikátor

NVIDIA GPU Display Driver - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0071 sa nachádza v produkte NVIDIA GPU Display Driver pre Windows, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0073 sa nachádza v produkte NVIDIA GPU Display Driver for Windows, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v komponente jadra produktu a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0077 sa nachádza v produkte NVIDIA Virtual GPU Manager, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v plugine vGPU a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.2.2024

CVE

CVE-2024-0071, CVE-2024-0073, CVE-2024-0074, CVE-2024-0078, CVE-2024-0075, CVE-2022-42265, CVE-2024-0077, CVE-024-0079

Zasiahnuté systémy

NVIDIA GPU Display Driver
NVIDIA Virtual GPU Manager

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

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

Zdroje

https://nvidia.custhelp.com/app/answers/detail/a_id/5520

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

Identifikátor

Santesoft Sante DICOM Viewer Pro - bezpečnostná zraniteľnosť

Popis

Spoločnosť Santesoft vydala bezpečnostnú aktualizáciu na svoj produkt Sante DICOM Viewer Pro, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených DICOM súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

27.2.2024

CVE

CVE-2024-1453

Zasiahnuté systémy

Sante DICOM Viewer Pro vo verzii staršej ako v14.0.4

Následky

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

Zdroje

https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-058-01

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

Identifikátor

MicroDicom DICOM Viewer - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť MicroDicom vydala bezpečnostnú aktualizáciu na svoj produkt ktorá opravuje dve bezpečnostné zraniteľnosti.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-22100 sa nachádza v produkte DICOM Viewer, 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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25578 sa nachádza v produkte DICOM Viewer, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

29.2.2024

CVE

CVE-2024-22100, CVE-2024-25578

Zasiahnuté systémy

MicroDicom DICOM viewer vo verzii staršej ako 2024.1

Následky

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

Zdroje

https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-060-01
https://www.microdicom.com/news/214-february-26-2024-new-version-dicom-viewer.html

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

Identifikátor

Delta Electronics CNCSoft-B - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Electronics vydala bezpečnosnú aktualizáciu svojho produktu CNCSoft-B, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1941 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. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

29.3.2024

CVE

CVE-2024-1941

Zasiahnuté systémy

CNCSoft-B V1.0.0.4 vo verzii staršej ako 2024-01-23

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.
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.cisa.gov/news-events/ics-advisories/icsa-24-060-01

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

Identifikátor

NI produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť NI vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti s identifikátormi CVE-2024-1155 a CVE-2024-1156 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

19.2.2024

CVE

CVE-2024-1155, CVE-2024-1156

Zasiahnuté systémy

SystemLink Server 2023
FlexLogger 2022 Q3
G Web Development Software
Static Test Software Suite
LabVIEW NXG 5.1 Web Module
LabVIEW NXG 5.1 Real-Time Module
LabVIEW NXG 5.1 Community Edition
Data Record AD
STS Software Bundle
Specification Compliance Manager

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

Eskalácia privilégií
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 je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch v sekcii ZDROJE.

Zdroje

https://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/incorrect-permissions-for-shared-systemlink-elixir-based-service.html
https://nvd.nist.gov/vuln/detail/CVE-2024-1155
https://nvd.nist.gov/vuln/detail/CVE-2024-1156

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:** 7.5
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM MQ - bezpečnostná zraniteľnosť

Popis

Spoločnosť IBM vydala bezpečnostnú aktualizáciu na svoj produkt IBM MQ, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25016 sa nachádza v produkte IBM MQ, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

3.3.2024

CVE

CVE-2024-25016

Zasiahnuté systémy

IBM MQ vo verzii staršej ako 9.0.0.23 LTS
IBM MQ vo verzii staršej ako 9.1.0.20 LTS
IBM MQ vo verzii staršej ako 9.2.0.22 LTS
IBM MQ vo verzii staršej ako 9.3.0.16 LTS
IBM MQ vo verzii staršej ako 9.3.5 CD

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/281279
https://www.ibm.com/support/pages/node/7123139?_ga=2.28825148.1630684636.1709538657-1003681650.1709024964
https://nvd.nist.gov/vuln/detail/CVE-2024-25016

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WordPress Giveaway and Contest - bezpečnostná zraniteľnosť

Popis

Vývojári WP pluginu RafflePress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1935 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom stored cross-site scripting (XSS) útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

29.2.2024

CVE

CVE-2024-1935

Zasiahnuté systémy

Giveaways and Contests by RafflePress vo verzii staršej ako 1.12.7

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/rafflepress/giveaways-and-contests-by-rafflepress-1125-unauthenticated-stored-cross-site-scripting
https://wordpress.org/plugins/rafflepress/

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:** 7.2
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WordPress AWeber plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu AWeber vydali bezpečnostnú aktualizáciu na svoj produkt, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1793 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom SQL injekcie vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

29.3.2024

CVE

CVE-2024-1793

Zasiahnuté systémy

AWeber vo verzii staršej ako 7.3.15

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/aweber-web-form-widget/aweber-free-sign-up-form-and-landing-page-builder-plugin-for-lead-generation-and-email-newsletter-growth-by-aweber-7314-authenticated-admin-sql-injection

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BEZPEČNOSTNÝ BULLETIN

Týždeň 28. 02. 2024 - 05. 03. 2024

No: B20240305-22V

22 / 22

Dôležitosť	☐ **Nízka**	■ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric MELSEC iQ-F Series - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti riadiacich systémov série MELSEC iQ-F od výrobcu Mitsubishi Electric.

Bezpečnostná zraniteľnosť s identifikátorom CVE-2023-7033 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov (TCP SYN Flood útok) spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.2.2024

CVE

CVE-2023-7033

Zasiahnuté systémy

MELSEC iQ-F FX5U-32MT/ES: vo všetkých verziách
MELSEC iQ-F FX5U-32MT/DS: vo všetkých verziách
MELSEC iQ-F FX5U-32MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5U-32MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5U-32MR/ES: vo všetkých verziách
MELSEC iQ-F FX5U-32MR/DS: vo všetkých verziách
MELSEC iQ-F FX5U-64MT/ES: vo všetkých verziách
MELSEC iQ-F FX5U-64MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5U-64MT/DS: vo všetkých verziách
MELSEC iQ-F FX5U-64MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5U-64MR/ES: vo všetkých verziách
MELSEC iQ-F FX5U-64MR/DS: vo všetkých verziách
MELSEC iQ-F FX5U-80MT/ES: vo všetkých verziách
MELSEC iQ-F FX5U-80MT/DS: vo všetkých verziách
MELSEC iQ-F FX5U-80MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5U-80MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5U-80MR/ES: vo všetkých verziách
MELSEC iQ-F FX5U-80MR/DS: vo všetkých verziách
MELSEC iQ-F FX5UC-32MT/D: vo všetkých verziách
MELSEC iQ-F FX5UC-32MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5UC-64MT/D: vo všetkých verziách
MELSEC iQ-F FX5UC-64MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5UC-96MT/D: vo všetkých verziách
MELSEC iQ-F FX5UC-96MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5UC-32MT/DS-TS: vo všetkých verziách
MELSEC iQ-F FX5UC-32MT/DSS-TS: vo všetkých verziách
MELSEC iQ-F FX5UC-32MR/DS-TS: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MT/ES: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MT/DS: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MR/ES: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MR/DS: vo všetkých verziách
MELSEC iQ-F FX5UJ-40MT/ES: vo všetkých verziách
MELSEC iQ-F FX5UJ-40MT/DS: vo všetkých verziách

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

MELSEC iQ-F FX5UJ-40MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5UJ-40MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5UJ-40MR/ES: vo všetkých verziách
MELSEC iQ-F FX5UJ-40MR/DS: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MT/ES: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MT/DS: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MT/DSS: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MR/ES: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MR/DS: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MT/ES-A*: vo všetkých verziách
MELSEC iQ-F FX5UJ-24MR/ES-A*: vo všetkých verziách
MELSEC iQ-F FX5UJ-40MT/ES-A*: vo všetkých verziách
MELSEC iQ-F FX5UJ-40MR/ES-A*: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MT/ES-A*: vo všetkých verziách
MELSEC iQ-F FX5UJ-60MR/ES-A*: vo všetkých verziách
MELSEC iQ-F FX5S-30MT/ES: vo všetkých verziách
MELSEC iQ-F FX5S-30MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5S-30MR/ES: vo všetkých verziách
MELSEC iQ-F FX5S-40MT/ES: vo všetkých verziách
MELSEC iQ-F FX5S-40MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5S-40MR/ES: vo všetkých verziách
MELSEC iQ-F FX5S-60MT/ES: vo všetkých verziách
MELSEC iQ-F FX5S-60MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5S-60MR/ES: vo všetkých verziách
MELSEC iQ-F FX5S-80*MT/ES: vo všetkých verziách
MELSEC iQ-F FX5S-80*MT/ESS: vo všetkých verziách
MELSEC iQ-F FX5S-80*MR/ES: vo všetkých verziách

Následky

Zneprístupnenie služby

Odporúčania

Vzhľadom na absenciu záplat pre danú zraniteľnosť odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, detailné inštrukcie môžete nájsť na webovej adrese:
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-023_en.pdf
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.cisa.gov/news-events/ics-advisories/icsa-24-058-01
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-023_en.pdf