BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 03. 2024 - 26. 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

GamiPress WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári GamiPress pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1799 v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.3.2024

CVE

CVE-2024-1799

Zasiahnuté systémy

GamiPress vo verzii staršej ako 6.8.7

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 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/gamipress/gamipress-the-1-gamification-plugin-to-reward-points-achievements-badges-ranks-in-wordpress-686-authenticated-contributor-sql-injection-via-shortcode

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

Identifikátor

Bosch Network Synchronizer - bezpečnostná zraniteľnosť

Popis

Spoločnosť BOSCH vydala bezpečnostnú aktualizáciu na svoj produkt Bosch Network Synchronizer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25002 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

20.3.2024

CVE

CVE-2024-25002

Zasiahnuté systémy

Bosch Network Synchronizer vo verzii staršej ako 9.30.52153

Následky

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.
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.

Na aplikáciu aktuálnej verzie Bosch Network Synchronizer je potrebný nástroj 9.30 OMNEO Firmware Upload Tool. Detailné inštrukcie aplikácie záplaty, vrátane mitigácií, môžete nájsť na webovej adrese: https://psirt.bosch.com/security-advisories/bosch-sa-152190-bt.html

Zdroje

https://psirt.bosch.com/security-advisories/bosch-sa-152190-bt.html

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

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2625 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.3.2024

CVE

CVE-2024-2625, CVE-2024-2626, CVE-2024-2627, CVE-2024-2628, CVE-2024-2629, CVE-2024-2630, CVE-2024-2631

Zasiahnuté systémy

Chrome pre Linux vo verzii staršej ako 123.0.6312.58
Chrome pre Windows a Mac vo verzii staršej ako 123.0.6312.58/.59

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/2024/03/stable-channel-update-for-desktop_19.html
https://www.tenable.com/cve/CVE-2024-2625

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

Identifikátor

File Manager WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári File Manager pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1538 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom Cross-Site Request Forgery (CSRF) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

20.3.2024

CVE

CVE-2024-1538

Zasiahnuté systémy

File Manager vo verzii staršej ako 7.2.5

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 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.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-file-manager/file-manager-724-cross-site-request-forgery-to-local-js-file-inclusion

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

Identifikátor

Mozilla Firefox - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje prehliadače Mozilla Firefox a Firefox ESR, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-29944 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Druhú bezpečnostnú zraniteľnosť možno zneužiť na neoprávnený prístup k citlivým údajom a neoprávnenú zmenu v systéme.
Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

22.3.2024

CVE

CVE-2024-29944, CVE-2024-29943

Zasiahnuté systémy

Firefox ESR vo verzii staršej ako 115.9.1
Firefox vo verzii staršej ako 124.0.1

Následky

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

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.
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/mfsa2024-15/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-16/
https://securityonline.info/cve-2024-29944-cve-2024-29943-firefox-pwn2own/
https://www.auscert.org.au/bulletins/ESB-2024.1744/

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

Identifikátor

sira EasyRange - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti produktu EasyRange.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-28131 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

25.3.2024

CVE

CVE-2024-28131

Zasiahnuté systémy

EasyRange vo verzii staršej ako 1.41 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Vzhľadom na absenciu aktualizácií mitigujúcich danú zraniteľnosť ako aj absenciu reakcie výrobcu na pokusy o nadviazanie kontaktu zo strany bezpečnostných výskumníkov, bezpečnostní výskumníci odporúčajú dočasne obmedziť interakciu s predmetnou aplikáciou.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://jvn.jp/en/jp/JVN13113728/index.html

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

Identifikátor

Easy Property Listings WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári Easy Property Listings pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1893 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.3.2024

CVE

CVE-2024-1893

Zasiahnuté systémy

Easy Property Listings plugin vo verzii staršej ako 3.5.3

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 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/easy-property-listings/easy-property-listings-352-authenticatedcontributor-sql-injection-via-shortcode

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

Identifikátor

Appointment Booking Calendar — Simply Schedule Appointments Booking WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári Appointment Booking Calendar — Simply Schedule Appointments Booking pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2342 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.

Dátum prvého zverejnenia varovania

21.3.2024

CVE

CVE-2024-2342

Zasiahnuté systémy

Appointment Booking Calendar — Simply Schedule Appointments Booking vo verzii staršej ako 1.6.7.9

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, 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/simply-schedule-appointments/appointment-booking-calendar-simply-schedule-appointments-booking-plugin-1677-authenticated-contributor-sql-injection-via-shortcode

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

Identifikátor

KDDI HGW BL1500HM - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť KDDI vydala bezpečnostnú aktualizáciu na svoj produkt HGW BL1500HM, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-28041 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

22.3.2024

CVE

CVE-2024-28041, CVE-2024-21865, CVE-2024-29071

Zasiahnuté systémy

HGW BL1500HM vo verzii firmvéru staršej ako 002.001.019.

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.
SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.

Zdroje

http://jvn.jp/en/vu/JVNVU93546510/index.html
https://nvd.nist.gov/vuln/detail/CVE-2024-28041

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:** 8.3
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Red Hat OpenShift GitOps - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Red Hat vydala bezpečnostnú aktualizáciu na svoj produkt OpenShift GitOps, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-22424 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov komponentu argo-cd 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.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.3.2024

CVE

CVE-2007-4559, CVE-2020-17049, CVE-2022-3094, CVE-2022-36227, CVE-2022-37434, CVE-2022-40897, CVE-2022-48337, CVE-2022-48339, CVE-2022-48468, CVE-2022-48560, CVE-2022-48564, CVE-2023-2602, CVE-2023-2603, CVE-2023-3446, CVE-2023-3817, CVE-2023-4016, CVE-2023-4641, CVE-2023-4806, CVE-2023-4813, CVE-2023-5455, CVE-2023-5678, CVE-2023-5981, CVE-2023-7104, CVE-2023-22745, CVE-2023-31486, CVE-2023-33460, CVE-2023-39615, CVE-2023-43804, CVE-2023-45803, CVE-2023-48795, CVE-2023-49568, CVE-2023-51385, CVE-2024-22424

Zasiahnuté systémy

Red Hat OpenShift GitOps 1.10 x86_64
Red Hat OpenShift GitOps 1.11 x86_64
Red Hat OpenShift GitOps 1.9 x86_64
Red Hat OpenShift GitOps for ARM 64 1.10 aarch64
Red Hat OpenShift GitOps for ARM 64 1.11 aarch64
Red Hat OpenShift GitOps for ARM 64 1.9 aarch64
Red Hat OpenShift GitOps for IBM Power, little endian 1.10 ppc64le
Red Hat OpenShift GitOps for IBM Power, little endian 1.11 ppc64le
Red Hat OpenShift GitOps for IBM Power, little endian 1.9 ppc64le
Red Hat OpenShift GitOps for IBM Z and LinuxONE 1.10 s390x
Red Hat OpenShift GitOps for IBM Z and LinuxONE 1.11 s390x
Red Hat OpenShift GitOps for IBM Z and LinuxONE 1.9 s390x

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

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.

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

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

Zdroje
https://access.redhat.com/errata/RHSA-2024:0692 https://access.redhat.com/errata/RHSA-2024:0691 https://access.redhat.com/errata/RHSA-2024:0689

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

Identifikátor

Spring Framework - bezpečnostná zraniteľnosť

Popis

Spoločnosť Spring vydala bezpečnostnú aktualizáciu na svoj produkt Spring Framework, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-22259 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zneužitia open redirect zraniteľnosti alebo Server-Side Request Forgery (SSRF) útoku získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

15.3.2024

CVE

CVE-2024-22259

Zasiahnuté systémy

Spring Framework vo verzii staršej ako 6.1.5
Spring Framework vo verzii staršej ako 6.0.18
Spring Framework vo verzii staršej ako 5.3.33

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://spring.io/security/cve-2024-22259
https://nvd.nist.gov/vuln/detail/CVE-2024-22259

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

Identifikátor

Ubuntu Graphviz - bezpečnostná zraniteľnosť

Popis

Vývojári Linux distribúcie Ubuntu vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú bezpečnostnú zraniteľnosť v implementácii balíka Graphviz.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2023-46045 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených config6a súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

21.3.2024

CVE

CVE-2023-46045

Zasiahnuté systémy

graphviz vo verzii staršej ako 2.42.2-6ubuntu0.1~esm1 (Ubuntu 22.04)
graphviz vo verzii staršej ako 2.42.2-3ubuntu0.1~esm2 (Ubuntu 20.04)
graphviz vo verzii staršej ako 2.40.1-2ubuntu0.1~esm2 (Ubuntu 18.04)
graphviz vo verzii staršej ako 2.38.0-12ubuntu2.1+esm2 (Ubuntu 16.04)
graphviz vo verzii staršej ako 2.36.0-0ubuntu3.2+esm2 (Ubuntu 14.04)

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://ubuntu.com/security/notices/USN-6708-1
https://nvd.nist.gov/vuln/detail/CVE-2023-46045

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

Identifikátor

Franklin Fueling System EVO 550, EVO 5000 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Franklin Fueling System vydala bezpečnostné aktualizácie na produkty EVO 550 a EVO 5000, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2442 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

19.3.2024

CVE

CVE-2024-2442

Zasiahnuté systémy

EVO 550 vo verzii staršej ako 2.26.3.8963
EVO 5000 vo verzii staršej ako 2.26.3.8963

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
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.
SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-079-01
https://nvd.nist.gov/vuln/detail/CVE-2024-2442
https://www.franklinfueling.com/en/landing-pages/firmware/evo550-5000-firmware/

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

Identifikátor

aiohttp - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku Aiohttp vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-23334 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky
získať neoprávnený prístup k citlivým údajom. Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

29.1.2024

CVE

CVE-2024-23334

Zasiahnuté systémy

aiohttp vo verzii staršej ako 3.9.2

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie nevyužívajú frameworky, knižnice, pluginy, SDK alebo moduly v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://github.com/aio-libs/aiohttp/security/advisories/GHSA-5h86-8mv2-jq9f
https://nvd.nist.gov/vuln/detail/CVE-2024-23334

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

Identifikátor

WP Compress – Image Optimizer WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WP Compress – Image Optimizer pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1934 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

21.3.2024

CVE

CVE-2024-1934

Zasiahnuté systémy

WP Compress – Image Optimizer plugin vo verzii staršej ako 6.11.11

Následky

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.

Zdroje

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-compress-image-optimizer/wp-compress-image-optimizer-61110-missing-authorization-to-unauthenticated-cdn-modification

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

Identifikátor

WooCommerce Cloak Affiliate Links WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WooCommerce Cloak Affiliate Links pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1308 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

20.3.2024

CVE

CVE-2024-1308

Zasiahnuté systémy

WooCommerce Cloak Affiliate Links plugin vo verzii staršej ako 1.0.34

Následky

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.

Zdroje

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/woocommerce-cloak-affiliate-links/woocommerce-cloak-affiliate-links-1033-missing-authorization-to-unauthenticated-permalink-modification

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

Identifikátor

LunarNight Laboratory WebProxy - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti produktu WebProxy.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-28033 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

25.3.2024

CVE

CVE-2024-28033

Zasiahnuté systémy

WebProxy vo verzii 1.7.8 a 1.7.9

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Vzhľadom na absenciu aktualizácií mitigujúcich danú zraniteľnosť ako aj absenciu reakcie výrobcu na pokusy o nadviazanie kontaktu zo strany bezpečnostných výskumníkov, bezpečnostní výskumníci odporúčajú dočasne obmedziť interakciu s predmetnou aplikáciou.
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://jvn.jp/en/jp/JVN22376992/index.html

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