BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 03. 2024 - 12. 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

Elite Booster for WooCommerce WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári Elite Booster for WooCommerce pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1986 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. Bezpečnostnú zraniteľnosť je možné zneužiť len vtedy, keď je prostredníctvom predmetného pluginu povolené nahrávať súbory používateľmi.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2024-1986

Zasiahnuté systémy

Booster Elite for WooCommerce vo verzii staršej ako 7.1.8

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/booster-elite-for-woocommerce/elite-booster-for-woocommerce-717-authenticated-subscriber-arbitrary-file-upload

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

Identifikátor

PDF Invoices and Packing Slips For WooCommerce WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári PDF Invoices and Packing Slips For WooCommerce pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1773 spočíva v nedostatočnom overovaní používateľských vstupov 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

6.3.2024

CVE

CVE-2024-1773

Zasiahnuté systémy

PDF Invoices and Packing Slips For WooCommerce vo verzii staršej ako 1.3.8

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/pdf-invoices-and-packing-slips-for-woocommerce/pdf-invoices-and-packing-slips-for-woocommerce-137-authenticated-subscriber-php-object-injection
https://wordpress.org/plugins/pdf-invoices-and-packing-slips-for-woocommerce/

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

Identifikátor

Post Grid, Slider & Carousel Ultimate WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári Post Grid, Slider & Carousel Ultimate pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2006 sa sa nachádza v produkte Post Grid, Slider & Carousel Ultimate s doplnkom Shortcode, Gutenberg Block & Elementor Widget, 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

5.3.2024

CVE

CVE-2024-2006

Zasiahnuté systémy

Post Grid, Slider & Carousel Ultimate vo verzii staršej ako 1.6.8

Následky

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

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 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/post-grid-carousel-ultimate/post-grid-slider-carousel-ultimate-with-shortcode-gutenberg-block-elementor-widget-167-authenticated-contributor-php-object-injection-in-outpost-shortcode-metabox-markup
https://wordpress.org/plugins/post-grid-carousel-ultimate/

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

Identifikátor

Debian FontForge - viacero bezpečnostných zraniteľností

Popis

Vývojári distribúcie operačného systému Debian GNU/Linux vydali bezpečnostné aktualizácie svojho produktu, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2020-5496 sa nachádza v editore FontForge, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

8.3.2024

CVE

CVE-2020-5395, CVE-2020-5496, CVE-2024-25081, CVE-2024-25082

Zasiahnuté systémy

Debian 10 buster vo verzii staršej ako 1:20170731~dfsg-1+deb10u1.

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://lists.debian.org/debian-lts-announce/2024/03/msg00007.html
https://www.auscert.org.au/bulletins/ESB-2024.1484/

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

Identifikátor

Google Chrome - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Chrome, ktorá opravuje tri bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti s identifikátorom sa nachádzajú v produkte Chrome, spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov v komponente V8 a umožňujú 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

5.3.2024

CVE

CVE-2024-2173, CVE-2024-2174, CVE-2024-2176

Zasiahnuté systémy

Google Chrome pre Windows a Mac vo verzii staršej ako 122.0.6261.111/.112
Google Chrome pre Linux vo verzii staršej ako 122.0.6261.111 (bezpečnostná záplata bude dostupná v nasledovných 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/2024/03/stable-channel-update-for-desktop.html
https://www.tenable.com/cve/CVE-2024-2173
https://www.tenable.com/cve/CVE-2024-2174
https://www.tenable.com/cve/CVE-2024-2176

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

Identifikátor

Restaurant Reservations WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári Restaurant Reservations pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1382 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorených súborov eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2024-1382

Zasiahnuté systémy

Restaurant Reservations vo verzii staršej ako 2.0

Následky

Vykonanie škodlivého kódu
Eskalácia privilégií
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/nd-restaurant-reservations/restaurant-reservations-19-directory-traversal-to-authenticated-contributor-local-file-inclusion

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
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.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-20337 sa nachádza v produkte Cisco Secure Client, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného odkazu získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.
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

6.3.2024

CVE

CVE-2024-20337, CVE-2024-20338, CVE-2024-20345, CVE-2024-20346, CVE-2024-20292, CVE-2024-20301, CVE-2024-20335, CVE-2024-20336

Zasiahnuté systémy

Secure Client pre Linux
Secure Client pre macOS
Secure Client pre Windows
Secure Client pre mobilné zariadenia s operačným systémom iOS, Android, alebo Universal Windows Platform
Cisco AppDynamics Controller Cloud
Cisco AppDynamics Controller On-Premise
Cisco Duo Authentication pre Windows Logon a RDP
Cisco Small Business 100 Series Wireless AP vo všetkých verziách (ukončená podpora)
Cisco Small Business 300 Series Wireless AP vo všetkých verziách (ukončená podpora)
Cisco Small Business 500 Series Wireless AP vo všetkých verziách (ukončená podpora)

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch 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.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Vzhľadom na to, že produkty série Cisco Small Business 100, 300 a 500 už nie sú udržiavané, v ich prípade odporúčame prejsť na iný produkt s platnou podporou.

Zdroje

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-client-crlf-W43V4G7
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-privesc-sYxQO6ds

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

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-traversal-m7N8mZpF
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-xss-3JwqSMNT
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-infodisc-rLCEqm6T
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-win-bypass-pn42KKBm
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-85G83CRB

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
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.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2022-46329 sa nachádza v produkte Red Hat Enterprise Linux, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

5.3.2024

CVE

CVE-2020-12762, CVE-2022-41973, CVE-2022-46329, CVE-2022-4899, CVE-2023-20592, CVE-2023-21911, CVE-2023-21919, CVE-2023-21920, CVE-2023-21929, CVE-2023-21933, CVE-2023-21935, CVE-2023-21940, CVE-2023-21945, CVE-2023-21946, CVE-2023-21947, CVE-2023-21953, CVE-2023-21955, CVE-2023-21962, CVE-2023-21966, CVE-2023-21972, CVE-2023-21976, CVE-2023-21977, CVE-2023-21980, CVE-2023-21982, CVE-2023-22005, CVE-2023-22007, CVE-2023-22008, CVE-2023-22032, CVE-2023-22033, CVE-2023-22038, CVE-2023-22046, CVE-2023-22048, CVE-2023-22053, CVE-2023-22054, CVE-2023-22056, CVE-2023-22057, CVE-2023-22058, CVE-2023-22059, CVE-2023-22064, CVE-2023-22065, CVE-2023-22066, CVE-2023-22068, CVE-2023-22070, CVE-2023-22078, CVE-2023-22079, CVE-2023-22084, CVE-2023-22092, CVE-2023-22097, CVE-2023-22103, CVE-2023-22104, CVE-2023-22110, CVE-2023-22111, CVE-2023-22112, CVE-2023-22113, CVE-2023-22114, CVE-2023-22115, CVE-2023-32324, CVE-2023-34241, CVE-2023-39326, CVE-2023-40225, CVE-2023-45285, CVE-2023-45539, CVE-2023-46589, CVE-2024-20960, CVE-2024-20961, CVE-2024-20962, CVE-2024-20963, CVE-2024-20964, CVE-2024-20965, CVE-2024-20966, CVE-2024-20967, CVE-2024-20968, CVE-2024-20969, CVE-2024-2097, CVE-2024-20970, CVE-2024-20971, CVE-2024-20972, CVE-2024-20973, CVE-2024-20974, CVE-2024-20976, CVE-2024-20977, CVE-2024-20978, CVE-2024-20981, CVE-2024-20982, CVE-2024-20983, CVE-2024-20984, CVE-2024-20985

Zasiahnuté systémy

Red Hat Enterprise Linux AppStream EUS
Red Hat CodeReady Linux Builder
Red Hat Enterprise Linux AppStream
Red Hat Enterprise Linux BaseOS EUS

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

Zdroje

https://access.redhat.com/errata/RHSA-2024:1112
https://access.redhat.com/errata/RHSA-2024:1154

https://access.redhat.com/errata/RHSA-2024:1142
https://access.redhat.com/errata/RHSA-2024:1141
https://access.redhat.com/errata/RHSA-2024:1134
https://access.redhat.com/errata/RHSA-2024:1131
https://access.redhat.com/errata/RHSA-2024:1110
https://access.redhat.com/errata/RHSA-2024:1101

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

Identifikátor

Post Form – Registration Form – Profile Form for User Profiles – Frontend Content Forms for User Submissions (UGC) WP plugin - tri bezpečnostné zraniteľnosti

Popis

Vývojári Post Form – Registration Form – Profile Form for User Profiles – Frontend Content Forms for User Submissions (UGC) pluginu pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1170 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

6.3.2024

CVE

CVE-2024-1170, CVE-2024-1169, CVE-2024-1158

Zasiahnuté systémy

Post Form – Registration Form – Profile Form for User Profiles – Frontend Content Forms for User Submissions (UGC) vo verzii staršej ako 2.8.8

Následky

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.

Zdroje

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/buddyforms/post-form-registration-form-profile-form-for-user-profiles-frontend-content-forms-for-user-submissions-ugc-287-missing-authorization-to-unauthenticated-media-deletion
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/buddyforms/post-form-registration-form-profile-form-for-user-profiles-frontend-content-forms-for-user-submissions-ugc-287-missing-authorization-to-unauthenticated-media-upload
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/buddyforms/post-form-registration-form-profile-form-for-user-profiles-frontend-content-forms-for-user-submissions-ugc-287-missing-authorization

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

Identifikátor

WooCommerce Add to Cart WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu WooCommerce Add to Cart vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2024-1862 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2024-1862

Zasiahnuté systémy

WooCommerce Add to Cart plugin vo verzii staršej ako 1.2.14

Následky

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.

Zdroje

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/woocommerce-add-to-cart-custom-redirect/woocommerce-add-to-cart-custom-redirect-1213-authenticatedcontributor-missing-authorization-to-limited-arbitrary-options-update

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 03. 2024 - 12. 03. 2024

No: B20240312-11V

11 / 25

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

Identifikátor

Dell iDRAC8 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt iDRAC8, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť identifikátorom CVE-2024-25951 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

8.3.2024

CVE

CVE-2024-25951

Zasiahnuté systémy

iDRAC8 vo verzii staršej ako 2.85.85.85

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://exchange.xforce.ibmcloud.com/vulnerabilities/285240
https://www.dell.com/support/kbdoc/en-us/000222591/dsa-2024-089-security-update-for-dell-idrac8-local-racadm-vulnerability

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:** 7.8
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Ashlar-Vellum Cobalt - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o šiestich zero day zraniteľnostiach v produkte spoločnosti Ashlar-Vellum.
Bezpečnostné zraniteľnosti sa nachádzajú v produkte Cobalt, spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených
STP a IGS súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľností vyžaduje interakciu používateľa.
Zraniteľnostiam nebol pridelený identifikátor CVE.

Dátum prvého zverejnenia varovania

28.2.2024

CVE

Zasiahnuté systémy

Cobalt vo všetkých verziách

Následky

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

Odporúčania

Vzhľadom na absenciu záplat pre predmetné zraniteľnosti odporúčame administrátorom sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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.zerodayinitiative.com/advisories/ZDI-24-239/
https://www.zerodayinitiative.com/advisories/ZDI-24-234/
https://www.zerodayinitiative.com/advisories/ZDI-24-247/
https://www.zerodayinitiative.com/advisories/ZDI-24-246/
https://www.zerodayinitiative.com/advisories/ZDI-24-249/
https://www.zerodayinitiative.com/advisories/ZDI-24-248/

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:** 7.8
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SKYSEA Client View - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Sky vydala bezpečnostnú aktualizáciu na svoj produkt SKYSEA Client View, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-24964 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2024-24964, CVE-2024-21805

Zasiahnuté systémy

SKYSEA Client View vo verzii staršej ako 19.2

Následky

Eskalácia privilégií
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 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://jvn.jp/en/jp/JVN54451757/index.html

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

Identifikátor

Santesoft Sante FFT Imaging - bezpečnostná zraniteľnosť

Popis

Spoločnosť Santesoft vydala bezpečnostnú aktualizáciu na svoj produkt Sante FFT Imaging, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1696 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených DCM súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

5.3.2024

CVE

CVE-2024-1696

Zasiahnuté systémy

Sante FFT Imaging vo verzii staršej ako v1.4.2

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://santesoft.com/win/sante-fft-imaging/download.html
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-065-01

BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 03. 2024 - 12. 03. 2024

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
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-2024-25744 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód alebo spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na vykonanie škodlivého kódu, neoprávnený prístup k citlivým údajom, neoprávenú zmenu v systéme, zneprístupnenie služby a eskaláciu privilégií.

Dátum prvého zverejnenia varovania

4.3.2024

CVE

CVE-2024-0741, CVE-2024-0742, CVE-2024-0747, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0755, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1553, CVE-2024-1936, CVE-2024-0746, CVE-2024-1546, CVE-2024-1551, CVE-2024-1552, CVE-2023-23919, CVE-2023-23920, CVE-2023-2650, CVE-2024-26130, CVE-2023-50782, CVE-2024-27351, CVE-2022-24720, CVE-2023-49468, CVE-2023-49465, CVE-2023-27102, CVE-2023-49467, CVE-2023-27103, CVE-2023-47471, CVE-2023-43887, CVE-2024-24575, CVE-2024-24577, CVE-2020-12278, CVE-2023-22742, CVE-2020-12279, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1553, CVE-2024-1554, CVE-2024-1555, CVE-2024-1557, CVE-2024-1546, CVE-2024-1551, CVE-2024-1552, CVE-2024-1556, CVE-2024-27913, CVE-2023-46343, CVE-2023-51782, CVE-2023-6121, CVE-2023-51779, CVE-2024-0607, CVE-2023-6560, CVE-2024-25744, CVE-2023-22995, CVE-2023-51780, CVE-2021-44879, CVE-2023-51782, CVE-2024-0340, CVE-2023-6121, CVE-2023-4244, CVE-2023-51779, CVE-2024-21647, CVE-2020-11076, CVE-2023-40175, CVE-2020-11077, CVE-2022-23634, CVE-2022-24790, CVE-2023-34624, CVE-2023-50495, CVE-2019-0222, CVE-2023-4134, CVE-2023-6121, CVE-2024-0340, CVE-2023-51779, CVE-2024-0607, CVE-2023-46343, CVE-2023-51782, CVE-2023-22995, CVE-2023-46862, CVE-2023-46343, CVE-2024-0607, CVE-2023-6121, CVE-2024-25744, CVE-2023-51779, CVE-2023-51782, CVE-2023-6560

Zasiahnuté systémy

Ubuntu 23.10
thunderbird vo verzii staršej ako 1:115.8.1+build1-0ubuntu0.23.10.1
libnode108 vo verzii staršej ako 18.13.0+dfsg1-1ubuntu2.1
nodejs vo verzii staršej ako 18.13.0+dfsg1-1ubuntu2.1
python3-cryptography vo verzii staršej ako 38.0.4-4ubuntu0.23.10.2
python3-django vo verzii staršej ako 3:4.2.4-1ubuntu2.2
libde265-0 vo verzii staršej ako 1.0.12-2ubuntu0.1
libgit2-1.5 vo verzii staršej ako 1.5.1+ds-1ubuntu1.1
libc-ares2 vo verzii staršej ako 1.19.1-3ubuntu0.1
frr vo verzii staršej ako 8.4.4-1.1ubuntu1.3
linux-image-6.5.0-1016-azure vo verzii staršej ako 6.5.0-1016.16
linux-image-6.5.0-1016-azure-fde vo verzii staršej ako 6.5.0-1016.16
linux-image-azure vo verzii staršej ako 6.5.0.1016.18
linux-image-azure-fde vo verzii staršej ako 6.5.0.1016.18

Ubuntu 22.04
thunderbird vo verzii staršej ako 1:115.8.1+build1-0ubuntu0.22.04.1
libnode72 vo verzii staršej ako 12.22.9~dfsg-1ubuntu3.4
nodejs vo verzii staršej ako 12.22.9~dfsg-1ubuntu3.4
python3-cryptography vo verzii staršej ako 3.4.8-1ubuntu2.2
python3-django vo verzii staršej ako 2:3.2.12-2ubuntu1.11

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

ruby-image-processing vo verzii staršej ako 1.10.3-1ubuntu0.22.04.1
libde265-0 vo verzii staršej ako 1.0.8-1ubuntu0.3
libgit2-1.1 vo verzii staršej ako 1.1.0+dfsg.1-4.1ubuntu0.1
libc-ares2 vo verzii staršej ako 1.18.1-1ubuntu0.22.04.3
frr vo verzii staršej ako 8.1-1ubuntu1.9
puma vo verzii staršej ako 5.5.2-2ubuntu2+esm1
libhtmlcleaner-java vo verzii staršej ako 2.24-1+deb11u1build0.22.04.1
linux-image-5.15.0-100-generic vo verzii staršej ako 5.15.0-100.110
linux-image-5.15.0-100-generic-64k vo verzii staršej ako 5.15.0-100.110
linux-image-5.15.0-100-generic-lpae vo verzii staršej ako 5.15.0-100.110
linux-image-5.15.0-1038-gkeop vo verzii staršej ako 5.15.0-1038.44
linux-image-5.15.0-1046-nvidia vo verzii staršej ako 5.15.0-1046.46
linux-image-5.15.0-1046-nvidia-lowlatency vo verzii staršej ako 5.15.0-1046.46
linux-image-5.15.0-1048-ibm vo verzii staršej ako 5.15.0-1048.51
linux-image-5.15.0-1052-gke vo verzii staršej ako 5.15.0-1052.57
linux-image-5.15.0-1053-gcp vo verzii staršej ako 5.15.0-1053.61
linux-image-5.15.0-1058-azure vo verzii staršej ako 5.15.0-1058.66
linux-image-5.15.0-1058-azure-fde vo verzii staršej ako 5.15.0-1058.66.1
linux-image-azure-fde-lts-22.04 vo verzii staršej ako 5.15.0.1058.66.36
linux-image-azure-lts-22.04 vo verzii staršej ako 5.15.0.1058.54
linux-image-gcp-lts-22.04 vo verzii staršej ako 5.15.0.1053.49
linux-image-generic vo verzii staršej ako 5.15.0.100.97
linux-image-generic-64k vo verzii staršej ako 5.15.0.100.97
linux-image-generic-lpae vo verzii staršej ako 5.15.0.100.97
linux-image-gke vo verzii staršej ako 5.15.0.1052.51
linux-image-gke-5.15 vo verzii staršej ako 5.15.0.1052.51
linux-image-gkeop vo verzii staršej ako 5.15.0.1038.37
linux-image-gkeop-5.15 vo verzii staršej ako 5.15.0.1038.37
linux-image-ibm vo verzii staršej ako 5.15.0.1048.44
linux-image-nvidia vo verzii staršej ako 5.15.0.1046.46
linux-image-nvidia-lowlatency vo verzii staršej ako 5.15.0.1046.46
linux-image-virtual vo verzii staršej ako 5.15.0.100.97
linux-image-6.5.0-1016-azure vo verzii staršej ako 6.5.0-1016.16~22.04.1
linux-image-6.5.0-1016-azure-fde vo verzii staršej ako 6.5.0-1016.16~22.04.1
linux-image-6.5.0-25-generic vo verzii staršej ako 6.5.0-25.25~22.04.1
linux-image-6.5.0-25-generic-64k vo verzii staršej ako 6.5.0-25.25~22.04.1
linux-image-azure vo verzii staršej ako 6.5.0.1016.16~22.04.1
linux-image-azure-fde vo verzii staršej ako 6.5.0.1016.16~22.04.1
linux-image-generic-64k-hwe-22.04 vo verzii staršej ako 6.5.0.25.25~22.04.12
linux-image-generic-hwe-22.04 vo verzii staršej ako 6.5.0.25.25~22.04.12
linux-image-virtual-hwe-22.04 vo verzii staršej ako 6.5.0.25.25~22.04.12

Ubuntu 20.04
thunderbird vo verzii staršej ako 1:115.8.1+build1-0ubuntu0.20.04.1
libnode64 vo verzii staršej ako 10.19.0~dfsg-3ubuntu1.5
nodejs vo verzii staršej ako 10.19.0~dfsg-3ubuntu1.5
python-cryptography vo verzii staršej ako 2.8-3ubuntu0.3
python3-cryptography vo verzii staršej ako 2.8-3ubuntu0.3
python3-django vo verzii staršej ako 2:2.2.12-1ubuntu0.22
ruby-image-processing vo verzii staršej ako 1.10.3-1ubuntu0.20.04.1
libde265-0 vo verzii staršej ako 1.0.4-1ubuntu0.4
libgit2-28 vo verzii staršej ako 0.28.4+dfsg.1-2ubuntu0.1
firefox vo verzii staršej ako 123.0.1+build1-0ubuntu0.20.04.1
libc-ares2 vo verzii staršej ako 1.15.0-1ubuntu0.5
linux-image-5.4.0-1032-iot vo verzii staršej ako 5.4.0-1032.33
linux-image-5.4.0-1087-gkeop vo verzii staršej ako 5.4.0-1087.91
linux-image-5.4.0-1104-raspi vo verzii staršej ako 5.4.0-1104.116
linux-image-5.4.0-1108-kvm vo verzii staršej ako 5.4.0-1108.115
linux-image-5.4.0-1124-gcp vo verzii staršej ako 5.4.0-1124.133
linux-image-5.4.0-173-generic vo verzii staršej ako 5.4.0-173.191
linux-image-5.4.0-173-generic-lpae vo verzii staršej ako 5.4.0-173.191
linux-image-5.4.0-173-lowlatency vo verzii staršej ako 5.4.0-173.191

linux-image-gcp-lts-20.04 vo verzii staršej ako 5.4.0.1124.126
linux-image-generic vo verzii staršej ako 5.4.0.173.171
linux-image-generic-lpae vo verzii staršej ako 5.4.0.173.171
linux-image-gkeop vo verzii staršej ako 5.4.0.1087.85
linux-image-gkeop-5.4 vo verzii staršej ako 5.4.0.1087.85
linux-image-kvm vo verzii staršej ako 5.4.0.1108.104
linux-image-lowlatency vo verzii staršej ako 5.4.0.173.171
linux-image-oem vo verzii staršej ako 5.4.0.173.171
linux-image-oem-osp1 vo verzii staršej ako 5.4.0.173.171
linux-image-raspi vo verzii staršej ako 5.4.0.1104.134
linux-image-raspi2 vo verzii staršej ako 5.4.0.1104.134
linux-image-virtual vo verzii staršej ako 5.4.0.173.171
puma vo verzii staršej ako 3.12.4-1ubuntu2+esm1
libhtmlcleaner-java vo verzii staršej ako 2.23-1ubuntu0.1~esm1
libmqtt-client-java vo verzii staršej ako 1.14-1+deb10u1build0.20.04.1
linux-image-5.15.0-100-generic vo verzii staršej ako 5.15.0-100.110~20.04.1
linux-image-5.15.0-100-generic-64k vo verzii staršej ako 5.15.0-100.110~20.04.1
linux-image-5.15.0-100-generic-lpae vo verzii staršej ako 5.15.0-100.110~20.04.1
linux-image-5.15.0-100-lowlatency vo verzii staršej ako 5.15.0-100.110~20.04.1
linux-image-5.15.0-100-lowlatency-64k vo verzii staršej ako 5.15.0-100.110~20.04.1
linux-image-5.15.0-1038-gkeop vo verzii staršej ako 5.15.0-1038.44~20.04.1
linux-image-5.15.0-1048-ibm vo verzii staršej ako 5.15.0-1048.51~20.04.1
linux-image-5.15.0-1053-gcp vo verzii staršej ako 5.15.0-1053.61~20.04.1
linux-image-5.15.0-1058-azure vo verzii staršej ako 5.15.0-1058.66~20.04.2
linux-image-5.15.0-1058-azure-fde vo verzii staršej ako 5.15.0-1058.66~20.04.2.1
linux-image-azure vo verzii staršej ako 5.15.0.1058.66~20.04.48
linux-image-azure-cvm vo verzii staršej ako 5.15.0.1058.66~20.04.48
linux-image-azure-fde vo verzii staršej ako 5.15.0.1058.66~20.04.1.36
linux-image-gcp vo verzii staršej ako 5.15.0.1053.61~20.04.1
linux-image-generic-64k-hwe-20.04 vo verzii staršej ako 5.15.0.100.110~20.04.52
linux-image-generic-hwe-20.04 vo verzii staršej ako 5.15.0.100.110~20.04.52
linux-image-generic-lpae-hwe-20.04 vo verzii staršej ako 5.15.0.100.110~20.04.52
linux-image-gkeop-5.15 vo verzii staršej ako 5.15.0.1038.44~20.04.34
linux-image-ibm vo verzii staršej ako 5.15.0.1048.51~20.04.20
linux-image-lowlatency-64k-hwe-20.04 vo verzii staršej ako 5.15.0.100.110~20.04.49
linux-image-lowlatency-hwe-20.04 vo verzii staršej ako 5.15.0.100.110~20.04.49
linux-image-oem-20.04 vo verzii staršej ako 5.15.0.100.110~20.04.52
linux-image-oem-20.04b vo verzii staršej ako 5.15.0.100.110~20.04.52
linux-image-oem-20.04c vo verzii staršej ako 5.15.0.100.110~20.04.52
linux-image-oem-20.04d vo verzii staršej ako 5.15.0.100.110~20.04.52
linux-image-virtual-hwe-20.04 vo verzii staršej ako 5.15.0.100.110~20.04.52

Ubuntu 18.04
python-cryptography vo verzii staršej ako 2.1.4-1ubuntu1.4+esm1
python3-cryptography vo verzii staršej ako 2.1.4-1ubuntu1.4+esm1
python-django vo verzii staršej ako 1:1.11.11-1ubuntu1.21+esm4
python3-django vo verzii staršej ako 1:1.11.11-1ubuntu1.21+esm4
libde265-0 vo verzii staršej ako 1.0.2-2ubuntu0.18.04.1~esm4
libgit2-26 vo verzii staršej ako 0.26.0+dfsg.1-1.1ubuntu0.2+esm1
libc-ares2 vo verzii staršej ako 1.14.0-1ubuntu0.2+esm2
linux-image-5.4.0-1124-gcp vo verzii staršej ako 5.4.0-1124.133~18.04.1
linux-image-5.4.0-173-generic vo verzii staršej ako 5.4.0-173.191~18.04.1
linux-image-5.4.0-173-lowlatency vo verzii staršej ako 5.4.0-173.191~18.04.1
linux-image-gcp vo verzii staršej ako 5.4.0.1124.100
linux-image-generic-hwe-18.04 vo verzii staršej ako 5.4.0.173.191~18.04.141
linux-image-lowlatency-hwe-18.04 vo verzii staršej ako 5.4.0.173.191~18.04.141
linux-image-oem vo verzii staršej ako 5.4.0.173.191~18.04.141
linux-image-oem-osp1 vo verzii staršej ako 5.4.0.173.191~18.04.141
linux-image-snapdragon-hwe-18.04 vo verzii staršej ako 5.4.0.173.191~18.04.141
linux-image-virtual-hwe-18.04 vo verzii staršej ako 5.4.0.173.191~18.04.141
libhtmlcleaner-java vo verzii staršej ako 2.21-2ubuntu0.1~esm1
lib32ncurses5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2

lib32tinfo5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2
lib64ncurses5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2
lib64tinfo5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2
libncurses5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2
libtinfo5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2
libx32ncurses5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2
libx32tinfo5 vo verzii staršej ako 6.1-1ubuntu1.18.04.1+esm2

Ubuntu 16.04
libde265-0 vo verzii staršej ako 1.0.2-2ubuntu0.16.04.1~esm4
libgit2-24 vo verzii staršej ako 0.24.1-2ubuntu0.2+esm2
libc-ares2 vo verzii staršej ako 1.10.0-3ubuntu0.2+esm3
lib32ncurses5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5
lib32tinfo5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5
lib64ncurses5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5
lib64tinfo5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5
libncurses5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5
libtinfo5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5
libx32ncurses5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5
libx32tinfo5 vo verzii staršej ako 6.0+20160213-1ubuntu1+esm5

Ubuntu 14.04
lib32ncurses5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5
lib32tinfo5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5
lib64ncurses5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5
lib64tinfo5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5
libncurses5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5
libtinfo5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5
libx32ncurses5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5
libx32tinfo5 vo verzii staršej ako 5.9+20140118-1ubuntu1+esm5

Následky

Eskalácia privilégií
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 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.auscert.org.au/bulletins/ESB-2024.1499/
https://ubuntu.com/security/notices/USN-6672-1
https://ubuntu.com/security/notices/USN-6673-1
https://ubuntu.com/security/notices/USN-6674-1
https://ubuntu.com/security/notices/USN-6674-2
https://ubuntu.com/security/notices/USN-6675-1
https://ubuntu.com/security/notices/USN-6677-1
https://ubuntu.com/security/notices/USN-6678-1
https://ubuntu.com/security/notices/USN-6649-2
https://ubuntu.com/security/notices/USN-6676-1
https://ubuntu.com/security/notices/USN-6679-1
https://ubuntu.com/security/notices/USN-6680-1
https://ubuntu.com/security/notices/USN-6681-1
https://ubuntu.com/security/notices/USN-6682-1
https://ubuntu.com/security/notices/USN-6683-1
https://ubuntu.com/security/notices/USN-6684-1
https://ubuntu.com/security/notices/USN-6685-1
https://ubuntu.com/security/notices/USN-6686-1
https://ubuntu.com/security/notices/USN-6680-2
https://ubuntu.com/security/notices/USN-6669-1
https://exchange.xforce.ibmcloud.com/vulnerabilities/283669

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

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-23296 sa nachádza v produkte watchOS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitím ostatných bezpečnostných zraniteľností možno eskalovať svoje privilégiá a vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2022-42816, CVE-2022-48554, CVE-2023-28826, CVE-2023-42853, CVE-2023-48795, CVE-2023-51384 CVE-2023-51385, CVE-2024-0258, CVE-2024-23203, CVE-2024-23204, CVE-2024-23205, CVE-2024-23216, CVE-2024-23217, CVE-2024-23218, CVE-2024-23225, CVE-2024-23226, CVE-2024-23227, CVE-2024-23230, CVE-2024-23231, CVE-2024-23232, CVE-2024-23233, CVE-2024-23234, CVE-2024-23235, CVE-2024-23238, CVE-2024-23239, CVE-2024-23241, CVE-2024-23242, CVE-2024-23244, CVE-2024-23245, CVE-2024-23246, CVE-2024-23247, CVE-2024-23248, CVE-2024-23249, CVE-2024-23250, CVE-2024-23252, CVE-2024-23253, CVE-2024-23254, CVE-2024-23255, CVE-2024-23257, CVE-2024-23258, CVE-2024-23259, CVE-2024-23260, CVE-2024-23263, CVE-2024-23264, CVE-2024-23265, CVE-2024-23266, CVE-2024-23267, CVE-2024-23268, CVE-2024-23269 CVE-2024-23270, CVE-2024-23272, CVE-2024-23273, CVE-2024-23274, CVE-2024-23275, CVE-2024-23276, CVE-2024-23277, CVE-2024-23278, CVE-2024-23279, CVE-2024-23280, CVE-2024-23281, CVE-2024-23283, CVE-2024-23284, CVE-2024-23285, CVE-2024-23286, CVE-2024-23287, CVE-2024-23288, CVE-2024-23289, CVE-2024-23289, CVE-2024-23290, CVE-2024-23291, CVE-2024-23292, CVE-2024-23293, CVE-2024-23294, CVE-2024-23296, CVE-2024-23297

Zasiahnuté systémy

tvOS vo verzii staršej ako 17.4
watchOS vo verzii staršej ako 10.4
macOS Monterey vo verzii staršej ako 12.7.4
Safari vo verzii staršej ako 17.4
macOS Ventura vo verzii staršej ako 13.6.5
macOS Sonoma vo verzii staršej ako 14.4

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.

Zdroje

https://support.apple.com/en-au/HT214086
https://support.apple.com/en-gb/HT214088
https://support.apple.com/en-au/HT214083

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

https://support.apple.com/en-au/HT214089
https://support.apple.com/en-au/HT214085
https://support.apple.com/en-au/HT214084

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

Identifikátor

Dassault Systèmes eDrawings - bezpečnostná zraniteľnosť

Popis

Spoločnosť Dassault Systèmes vydala bezpečnostné aktualizácie na svoje produkty série eDrawings, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-1847 sa nachádza v produkte SOLIDWORKS, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného súboru (súbory typu: CATPART, DWG, DXF, IPT, JT, SAT, SLDDRW, SLDPRT, STL, STP, X_B or X_T) vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

8.3.2024

CVE

CVE-2024-1847

Zasiahnuté systémy

SOLIDWORKS 2023 vo verzii staršej ako SP5 (vrátane)
SOLIDWORKS 2024 vo verzii staršej ako SP1 (vrátane)

Bezpečnostnú záplatu môžete nájsť na webovej adrese výrobcu:
https://support.3ds.com/knowledge-base/?
q=docid:QA00000311982&_gl=1*1pu3dnb*_ga*ODE2OTU2NzQ5LjE3MTAxNTk1NjA.*_ga_DYJDKXYEZ4*MTcxMDE1OTU2MC4xLjEuMT

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.zerodayinitiative.com/advisories/ZDI-24-250/
https://nvd.nist.gov/vuln/detail/CVE-2024-1847
https://www.3ds.com/vulnerability/advisories

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 06. 03. 2024 - 12. 03. 2024

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

Identifikátor

GitLab (CE)/(EE) - dve bezpečnostné zraniteľnosti

Popis

Vývojári platformy GitLab vydali bezpečnostné aktualizácie svojich produktov GitLab Community Edition (CE) a GitLab Enterprise Edition (EE), ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0199 sa nachádza v produktoch GitLab (CE) a GitLab (EE), spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom neoprávnenej manipulácie s prístupovým tokenom eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

6.3.2024

CVE

CVE-2024-0199, CVE-2024-1299

Zasiahnuté systémy

GitLab Community Edition (CE) vo verzii staršej ako 16.9.2, 16.8.4 a 16.7.7
GitLab Enterprise Edition (EE) vo verzii staršej ako 16.9.2, 16.8.4 a 16.7.7

Následky

Eskalácia privilégií
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, 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://about.gitlab.com/releases/2024/03/06/security-release-gitlab-16-9-2-released/#guest-with-manage-group-access-tokens-can-rotate-and-see-group-access-token-with-owner-permissions

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 App Connect Enterprise/ Integration Bus - viacero bezpečnostných zraniteľností

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na produkty IBM App Connect Enterprise a IBM Integration Bus, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2023-33850 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom útoku postranným kanálom získať neoprávnený prístup k citlivým údajom.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

11.3.2024

CVE

CVE-2024-20919, CVE-2024-20952, CVE-2024-20945, CVE-2024-20926, CVE-2024-20921, CVE-2023-33850, CVE-2024-20918

Zasiahnuté systémy

IBM App Connect Enterprise vo verzii staršej ako 12.0.11.2
IBM App Connect Enterprise vo verzii staršej ako (vrátane) 11.0.0.24 - zraniteľnosť rieši bezpečnostná záplata IT45534
IBM Integration Bus vo verzii staršej ako (vrátane) 10.1.0.3 - zraniteľnosť rieši bezpečnostná záplata IT45534

Následky

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, 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/7130999

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

Identifikátor

Artica Proxy - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o bezpečnostnej zraniteľnosti produktu Artic Proxy.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2054 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód v kontexte používateľa www-data s následkom narušenia dôvernosti, integrity a dostupnosti systému. Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

5.3.2024

CVE

CVE-2024-2054

Zasiahnuté systémy

Artica Proxy vo verzii 4.50

Následky

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

Odporúčania

Vzhľadom na absenciu záplat pre predmetnú zraniteľnosť odporúčame administrátorom sledovať stránku výrobcu a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Pre dočasnú mitigáciu bezpečnostní výskumníci odporúčajú premiesniť alebo odstrániť adresár 'usr/share/artica-postfix/wizard'.
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://korelogic.com/Resources/Advisories/KL-001-2024-002.txt
https://www.redpacketsecurity.com/artica-proxy-code-execution-cve-2024-2054/
https://bnnbreaking.com/tech/cybersecurity/critical-security-alert-artica-proxy-hits-by-unauthenticated-php-deserialization-flaw

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

HPE Aruba Networking ArubaOS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť HPE Aruba Networking vydala bezpečnostné aktualizácie na svoj operačný systém ArubaOS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613, CVE-2024-25614, CVE-2024-25615, CVE-2024-25616

Zasiahnuté systémy

ArubaOS vo verzii staršej ako 10.5.1.0
ArubaOS vo verzii staršej ako 10.4.1.0
ArubaOS vo verzii staršej ako 8.11.2.1
ArubaOS vo verzii staršej ako 8.10.0.10

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. V prípade, že aktualizácia systému nie je možná, odporúčame postupovať podľa pokynov výrobcu uvedených na odkazoch 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.

Zdroje

https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04604en_us

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

Identifikátor

OMRON NJ/NX series - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktov spoločnosti OMRON.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-27121 sa nachádza v produktoch Machine Automation Controller série NJ a NX, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2024-27121

Zasiahnuté systémy

Machine Automation Controller NJ Series
Machine Automation Controller NX Series
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 odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Výrobca informuje, že bezpečnostné záplaty budú dostupné v priebehu apríla 2024.
Pre dočasnú mitigáciu odporúčame postupovať podľa pokynov výrobcu uvedených na webovej adrese: https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-001_en.pdf

Zdroje

https://jvn.jp/en/vu/JVNVU95852116/index.html
https://www.fa.omron.co.jp/product/security/assets/pdf/en/OMSR-2024-001_en.pdf

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

Identifikátor

Netgear RAX smerovače - bezpečnostná zraniteľnosť

Popis

Spoločnosť Netgear vydala bezpečnostnú aktualizáciu na svoje smerovače Netgear RAX, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2023-48725 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby. Na zneužitie zraniteľnosti potrebuje útočník poznať vaše heslo do siete Wi-Fi alebo mať zriadené ethernetové pripojenie k zariadeniu v sieti.

Dátum prvého zverejnenia varovania

7.3.2024

CVE

CVE-2023-48725

Zasiahnuté systémy

RAX28 vo verzii firmvéru staršieho ako 1.0.13.102_HOTFIX
RAX29 vo verzii firmvéru staršieho ako 1.0.13.102_HOTFIX
RAX30 vo verzii firmvéru staršieho ako 1.0.13.102_HOTFIX

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 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://kb.netgear.com/000066037/Security-Advisory-for-Post-Authentication-Stack-Overflow-on-the-RAX30-PSV-2023-0160
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1887
https://exchange.xforce.ibmcloud.com/vulnerabilities/284960

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 06. 03. 2024 - 12. 03. 2024

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

Identifikátor

Statistics WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu WP Statistics vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2194 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom stored cross-site scripting (stored XSS) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

11.3.2024

CVE

CVE-2024-2194

Zasiahnuté systémy

WP Statistics plugin vo verzii staršej ako 14.5.1

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, 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/wp-statistics/wp-statistics-145-unauthenticated-stored-cross-site-scripting

BEZPEČNOSTNÝ BULLETIN

Týždeň 06. 03. 2024 - 12. 03. 2024

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

Identifikátor

Zoom Rooms Client - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Zoom vydala bezpečnostnú aktualizáciu na svoj produkt Zoom Rooms Client, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-24693 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Bezpečnostnú zraniteľnosť s identifikátorom CVE-2024-24692 možno zneužiť na zneprístupnenie služby.
Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

12.3.2024

CVE

CVE-2024-24692, CVE-2024-24693

Zasiahnuté systémy

Zoom Rooms Client pre Windows vo verzii staršej ako 5.17.5

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.zoom.com/en/trust/security-bulletin/zsb-24010/
https://www.zoom.com/en/trust/security-bulletin/zsb-24009/