BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 04. 2024 - 16. 04. 2024

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: *sk-cert@nbu.gov.sk*
Mobil: *+421 903 993 706*
Tel: *+421 2 6869 2915*

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

BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 04. 2024 - 16. 04. 2024

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

Identifikátor

Microsoft produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje produkty, ktoré opravujú viacero bezpečnostných zraniteľností. Opravených bolo vyše 150 zraniteľností, z ktorých 67 umožňovalo vzdialené vykonanie kódu a 2 boli označené ako zero-day.

Zeor-day zraniteľnosť s označením CVE-2024-29988 v produktoch Windows a Windows Server spočíva v nesprávnom spracovaní .URL súborov, u ktorých nedochádzalo ku kontrole tzv. mark-of-the-web príznaku a vzdialený neautentifikovaný útočník by ju mohol zneužiť na obídenie SmartScreen ochrany a následné vykonanie škodlivého kódu.

Bezpečnostné zraniteľnosti s identifikátormi CVE-2024-29053 a CVE-2024-21323 sa nachádzajú v produkte Microsoft Defender for IoT, spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Zneužitím ostatných bezpečnostných zraniteľností možno eskalovať privilégiá, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

9.4.2024

CVE

CVE-2024-21409, CVE-2024-29993, CVE-2024-29063, CVE-2024-28917, CVE-2024-21424, CVE-2024-26193, CVE-2024-29989, CVE-2024-20685, CVE-2024-29992, CVE-2024-2201, CVE-2024-29988, CVE-2019-3816, CVE-2019-3833, CVE-2024-29990, CVE-2024-28905, CVE-2024-28907, CVE-2024-26213, CVE-2024-28904, CVE-2024-29055, CVE-2024-29053, CVE-2024-29054, CVE-2024-21324, CVE-2024-21323, CVE-2024-21322, CVE-2024-3156, CVE-2024-29049, CVE-2024-29981, CVE-2024-3159, CVE-2024-3158, CVE-2024-26158, CVE-2024-26257, CVE-2024-20670, CVE-2024-2625, CVE-2024-26214, CVE-2024-26244, CVE-2024-26210, CVE-2024-26233, CVE-2024-26231, CVE-2024-26227, CVE-2024-26223, CVE-2024-26221, CVE-2024-26224, CVE-2024-26222, CVE-2024-29064, CVE-2024-28937, CVE-2024-28938, CVE-2024-29044, CVE-2024-28935, CVE-2024-28940, CVE-2024-28943, CVE-2024-28941, CVE-2024-28944, CVE-2024-28909, CVE-2024-29985, CVE-2024-28906, CVE-2024-28933, CVE-2024-28934, CVE-2024-28927, CVE-2024-28930, CVE-2024-29046, CVE-2024-28932, CVE-2024-29047, CVE-2024-28931, CVE-2024-29984, CVE-2024-28929, CVE-2024-28939, CVE-2024-28942, CVE-2024-29043, CVE-2024-28936, CVE-2024-29045, CVE-2024-28915, CVE-2024-28913, CVE-2024-28945, CVE-2024-29048, CVE-2024-28912, CVE-2024-28914, CVE-2024-29983, CVE-2024-28911, CVE-2024-29982, CVE-2024-29056, CVE-2024-21447, CVE-2024-20665, CVE-2024-26256, CVE-2024-26228, CVE-2024-29050, CVE-2024-26237, CVE-2024-26212, CVE-2024-26215, CVE-2024-26195, CVE-2024-26202, CVE-2024-29066, CVE-2024-26226, CVE-2024-26172, CVE-2024-26216, CVE-2024-26219, CVE-2024-26253, CVE-2024-26252, CVE-2024-26183, CVE-2024-26248, CVE-2024-20693, CVE-2024-26245, CVE-2024-26229, CVE-2024-26218, CVE-2024-26209, CVE-2024-26232, CVE-2024-26208, CVE-2024-26220, CVE-2024-26234, CVE-2024-28902, CVE-2024-28900, CVE-2024-28901, CVE-2024-26255, CVE-2024-26230, CVE-2024-26239, CVE-2024-26207, CVE-2024-26217, CVE-2024-26211, CVE-2024-20678, CVE-2024-26200, CVE-2024-26179, CVE-2024-26205, CVE-2024-29061, CVE-2024-28921, CVE-2024-20689, CVE-2024-26250, CVE-2024-28922, CVE-2024-20669, CVE-2024-28898, CVE-2024-20688, CVE-2024-23593, CVE-2024-28896, CVE-2024-28919, CVE-2024-23594, CVE-2024-28923, CVE-2024-28903, CVE-2024-26189, CVE-2024-26240, CVE-2024-28924, CVE-2024-28897, CVE-2024-28925, CVE-2024-26175, CVE-2024-28920, CVE-2024-26194, CVE-2024-26180, CVE-2024-26171, CVE-2024-26168, CVE-2024-29052, CVE-2024-26242, CVE-2024-26236, CVE-2024-26235, CVE-2024-26243, CVE-2024-26241

Zasiahnuté systémy

.NET and Visual Studio
Azure
Azure AI Search
Azure Arc
Azure Compute Gallery
Azure Migrate
Azure Monitor

Azure Private 5G Core
Azure SDK
Internet Shortcut Files
Mariner
Microsoft Azure Kubernetes Service
Microsoft Brokering File System
Microsoft Defender for IoT
Microsoft Edge (Chromium-based)
Microsoft Install Service
Microsoft Office Excel
Microsoft Office Outlook
Microsoft Office SharePoint
Microsoft WDAC ODBC Driver
Microsoft WDAC OLE DB provider for SQL
Microsoft DNS Server
Microsoft Windows Hyper-V
SQL Server
Windows Authentication Methods
Windows BitLocker
Windows Compressed Folder
Windows Cryptographic Services
Windows Defender Credential Guard
Windows DHCP Server
Windows Distributed File System (DFS)
Windows DWM Core Library
Windows File Server Resource Management Service
Windows HTTP.sys
Windows Internet Connection Sharing (ICS)
Windows Kerberos
Windows Kernel
Windows Local Security Authority Subsystem Service (LSASS)
Windows Message Queuing
Windows Mobile Hotspot
Windows Proxy Driver
Windows Remote Access Connection Manager
Windows Remote Procedure Call
Windows Routing and Remote Access Service (RRAS)
Windows Secure Boot
Windows Storage
Windows Telephony Server
Windows Update Stack
Windows USB Print Driver
Windows Virtual Machine Bus
Windows Win32K - ICOMP

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.bleepingcomputer.com/microsoft-patch-tuesday-reports/Microsoft-Patch-Tuesday-April-2024.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/287029
https://exchange.xforce.ibmcloud.com/vulnerabilities/287109

https://msrc.microsoft.com/update-guide/releaseNote/2024-Apr

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

Identifikátor

Arista Edge Threat Management - Arista NG Firewall - bezpečnostná zraniteľnosť

Popis

Spoločnosť Arista vydala bezpečnostnú aktualizáciu na svoj produkt Arista Edge Threat Management - Arista NG Firewall, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-27889 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

9.4.2024

CVE

CVE-2024-27889

Zasiahnuté systémy

Arista Edge Threat Management - Arista NG Firewall vo verzii staršej ako 17.1

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. V prípade, že aktualizácia systému nie je možná, odporúčame zraniteľnosť mitigovať podľa odporúčaní od výrobcu. Detailné inštrukcie môžete nájsť na webovej adrese uvedenej v sekcii ZDROJE.
Rovnako odporúčame preveriť všetky dostupné logy na prítomnosť IOC a pokusov o zneužitie zraniteľnosti.
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.arista.com/en/support/advisories-notices/security-advisory/19038-security-advisory-0093
https://www.zerodayinitiative.com/advisories/ZDI-24-364/

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

Identifikátor

Google Chrome - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Google Chrome, ktorá opravuje tri bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sa nachádzajú v komponentoch Compositing, ANGLE a DAWN a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol znežiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

10.4.2024

CVE

CVE-2024-3157, CVE-2024-3516, CVE-2024-3515

Zasiahnuté systémy

Google Chrome pre Windows vo verzii staršej ako 123.0.6312.122/.123
Google Chrome pre Mac vo verzii staršej ako 123.0.6312.122/.123/.124
Google Chrome pre Linux vo verzii staršej ako 123.0.6312.122 (bezpečnostná záplata bude dostupná v nasledovných dňoch/ týždňoch)
Google Chrome pre Android vo verzii staršej ako 123.0.6312.118
Google ChromeOS a ChromeOS Flex vo verzii staršej ako 15786.48.0
Google Chrome Browser pre ChromeOS zariadenia verzii staršej ako 123.0.6312.112

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop_10.html
https://chromereleases.googleblog.com/2024/04/chrome-for-android-update_10.html
https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-chromeos-and.html

BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 04. 2024 - 16. 04. 2024

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

Identifikátor

Pluginy redakčného systému WordPress - viacero bezpečnostných zraniteľností

Popis

Vývojári pluginov pre redakčný systém WordPress vydali bezpečnostné aktualizácie svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2018 sa nachádza v plugine WP Activity Log Premium, 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.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

9.4.2024

CVE

CVE-2024-2018, CVE-2023-6964, CVE-2024-31355, CVE-2024-31370, CVE-2024-3020, CVE-2023-7046, CVE-2024-1774, CVE-2024-31356, CVE-2024-31365, CVE-2024-31366, CVE-2024-1956, CVE-2024-1292, CVE-2024-3048, CVE-2024-3076, CVE-2024-31358, CVE-2023-6811,

Zasiahnuté systémy

WP Activity Log Premium vo verzii staršej ako 4.6.4.1
Gutenberg Blocks by Kadence Blocks vo verzii staršej ako 3.2.12
Slideshow Gallery Plugin vo verzii staršej ako 1.7.8 (vrátane)
AIKit Plugin vo verzii staršej ako 4.14.1 (vrátane)
Carousel, Slider, Gallery by WP Carousel vo verzii staršej ako 2.6.4
WP Encryption – One Click Free SSL Certificate & SSL / HTTPS Redirect to Force HTTPS, SSL Score vo verzii staršej ako 7.1.0
Customily Product Personalizer vo verzii staršej ako 1.23.3 (vrátane)
User Activity Log Plugin vo verzii staršej ako 1.8 (vrátane)
Post Type Builder (PTB) vo verzii staršej ako 2.0.8 (vrátane)
WPB Show Core Plugin vo verzii staršej ako 2.7
WPB Show Core Plugin vo verzii staršej ako 2.6
Bannerlid Plugin vo verzii staršej ako 1.1.0 (vrátane)
MM-email2image Plugin vo verzii staršej ako 0.2.5 (vrátane)
5 Stars Rating Funnel Plugin vo verzii staršej ako 1.3.02
Language Translate Widget for WordPress vo verzii staršej ako 224
WordPress Core vo verzii staršej ako 6.1.6, 6.2.5, 6.3.4, 6.4.4, 6.5.2

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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 predmetné pluginy v zraniteľných verziách. V prípade, že áno, administrátorom SK-CERT odporúča:
– v prípade, že sa jedná o pluginy s ukončenou podporou, predmetné pluginy odinštalovať,
– v prípade, že sa jedná o pluginy, pre ktoré nie sú v súčasnosti dostupné bezpečnostné aktualizácie, predmetné pluginy až do vydania záplat deaktivovať alebo odinštalovať,
– v prípade, že sa jedná o pluginy, pre ktoré sú dostupné bezpečnostné záplaty, predmetné pluginy aktualizovať,

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

– vo všetkých prípadoch preveriť logy na prítomnosť pokusov o zneužitie zraniteľností,
– vo všetkých prípadoch preveriť integritu databázy a samotného redakčného systému.
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/wp-security-audit-log-premium/wp-activity-log-premium-464-authenticated-subscriber-sql-injection
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/kadence-blocks/gutenberg-blocks-by-kadence-blocks-page-builder-features-3126-authenticatedcontributor-server-side-request-forgery-ssrf
https://patchstack.com/database/vulnerability/slideshow-gallery/wordpress-slideshow-gallery-lite-plugin-1-7-8-sql-injection-vulnerability
https://patchstack.com/database/vulnerability/aikit-wordpress-ai-writing-assistant-using-gpt3/wordpress-codeisawesome-aikit-plugin-4-14-1-sql-injection-vulnerability
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-carousel-free/carousel-slider-gallery-by-wp-carousel-image-carousel-photo-gallery-post-carousel-post-grid-product-carousel-product-grid-for-woocommerce-263-authenticated-admin-php-object-injection
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-letsencrypt-ssl/wp-encryption-one-click-free-ssl-certificate-ssl-https-redirect-to-force-https-ssl-score-70-sensitive-information-exposure-via-insufficiently-protected-files
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/customily-v2/customily-product-personalizer-1233-unauthenticated-stored-cross-site-scripting
https://patchstack.com/database/vulnerability/user-activity-log/wordpress-user-activity-log-plugin-1-8-sql-injection-vulnerability
https://patchstack.com/database/vulnerability/themify-ptb/wordpress-post-type-builder-ptb-plugin-2-0-8-reflected-cross-site-scripting-xss-vulnerability
https://patchstack.com/database/vulnerability/themify-ptb/wordpress-post-type-builder-ptb-plugin-2-0-8-subscriber-arbitrary-post-page-creation-vulnerability
https://patchstack.com/database/vulnerability/wpb-show-core/wordpress-wpb-show-core-plugin-2-7-reflected-xss-vulnerability
https://patchstack.com/database/vulnerability/wpb-show-core/wordpress-wpb-show-core-plugin-2-6-reflected-xss-vulnerability
https://patchstack.com/database/vulnerability/bannerlid/wordpress-bannerlid-plugin-1-1-0-reflected-xss-vulnerability
https://patchstack.com/database/vulnerability/mm-email2image/wordpress-mm-email2image-plugin-0-2-5-stored-xss-via-csrf-vulnerability
https://patchstack.com/database/vulnerability/5-stars-rating-funnel/wordpress-5-stars-rating-funnel-plugin-1-2-67-arbitrary-content-deletion-vulnerability
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/conveythis-translate/language-translate-widget-for-wordpress-conveythis-223-unauthenticated-stored-cross-site-scripting-via-api-key
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-core/wordpress-core-652-authenticated-contributor-stored-cross-site-scripting-via-avatar-block?asset_slug=wordpress

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

Identifikátor

SUSE webkit2gtk3 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť SUSE vydala bezpečnostnú aktualizáciu na svoj produkt webkit2gtk3, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2023-42950 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na vykonanie škodlivého kódu, neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme a zneprístupnenie služby.
Zneužitie zraniteľností vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

15.4.2024

CVE

CVE-2024-23252, CVE-2024-23254, CVE-2024-23263, CVE-2024-23280, CVE-2024-23284, CVE-2023-42950, CVE-2023-42956, CVE-2023-42843

Zasiahnuté systémy

Basesystem Module 15-SP5
Desktop Applications Module 15-SP5
Development Tools Module 15-SP5
openSUSE Leap 15.4
openSUSE Leap 15.5
SUSE Enterprise Storage 7.1
SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4
SUSE Linux Enterprise Desktop 15 SP5
SUSE Linux Enterprise High Performance Computing 15 SP2
SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2
SUSE Linux Enterprise High Performance Computing 15 SP3
SUSE Linux Enterprise High Performance Computing 15 SP4
SUSE Linux Enterprise High Performance Computing 15 SP5
SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4
SUSE Linux Enterprise High Performance Computing LTSS 15 SP3
SUSE Linux Enterprise High Performance Computing LTSS 15 SP4
SUSE Linux Enterprise Real Time 15 SP5
SUSE Linux Enterprise Server 15 SP2
SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2
SUSE Linux Enterprise Server 15 SP3
SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3
SUSE Linux Enterprise Server 15 SP4
SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4
SUSE Linux Enterprise Server 15 SP5
SUSE Linux Enterprise Server for SAP Applications 15 SP2
SUSE Linux Enterprise Server for SAP Applications 15 SP3
SUSE Linux Enterprise Server for SAP Applications 15 SP4
SUSE Linux Enterprise Server for SAP Applications 15 SP5
SUSE Manager Proxy 4.3
SUSE Manager Retail Branch Server 4.3

SUSE Manager Server 4.3

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vzdialené vykonanie kódu, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.suse.com/support/update/announcement/2024/suse-su-20241269-1/
https://www.suse.com/support/update/announcement/2024/suse-su-20241270-1/

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

Identifikátor

Adobe Illustrator - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Adobe Illustrator, ktorá opravuje viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti s identifikátormi CVE-2024-30271, CVE-2024-30272 a CVE-2024-30273 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného dokumentu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

12.4.2024

CVE

CVE-2024-30271, CVE-2024-30272, CVE-2024-30273, CVE-2024-20798

Zasiahnuté systémy

Adobe Illustrator 2023 vo verzii staršej ako 27.9.3
Adobe Illustrator 2024 vo verzii staršej ako 28.4

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://helpx.adobe.com/security/products/illustrator/apsb24-25.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/287456
https://exchange.xforce.ibmcloud.com/vulnerabilities/287455
https://exchange.xforce.ibmcloud.com/vulnerabilities/287454

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

Identifikátor

Netdata - bezpečnostná zraniteľnosť

Popis

Vývojári open source monitorovacieho nástroja Netdata vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-32019 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvoreného súboru eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby. Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

11.4.2024

CVE

CVE-2024-32019

Zasiahnuté systémy

Netdata s balíčkom ndsudo vo verzii staršej ako v1.45.3, v1.45.0-169

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat 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://github.com/netdata/netdata/security/advisories/GHSA-pmhq-4cxq-wj93

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

Identifikátor

GitLab Community Edition (CE) a Enterprise Edition (EE) - štyri bezpečnostné zraniteľnosti

Popis

Vývojári platformy GitLab vydali bezpečnostné aktualizácie svojich produktov GitLab Community Edition (CE) a GitLab Enterprise Edition (EE), ktoré opravujú štyri bezpečnostné zraniteľnosti.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2024-3092 a CVE-2024-2279 spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom stored XSS (Stored Cross Site Scripting) útoku vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom alebo vykonať neoprávnené zmeny v systéme.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.4.2024

CVE

CVE-2024-3092, CVE-2024-2279, CVE-2023-6489, CVE-2023-6678

Zasiahnuté systémy

Gitlab Community Edition (CE) a Enterprise Edition (EE) vo verzii staršej ako 16.10.2, 16.9.4 a 16.8.6

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.
Následne odporúčame preveriť integritu kódu v repozitároch. Odporúčame tiež zaviesť podpisovanie commitov.

Zdroje

https://about.gitlab.com/releases/2024/04/10/patch-release-gitlab-16-10-2-released/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SUBNET Solutions PowerSYSTEM Server a Substation Server 2021 - bezpečnostná zraniteľnosť

Popis

Spoločnosť SUBNET Solutions vydala bezpečnostnú aktualizáciu na svoje produkty PowerSYSTEM Server a Substation Server 2021, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-3313 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať privilégiá na zasiahnutom systéme, spôsobiť zneprístupnenie služby a vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

9.4.2024

CVE

CVE-2024-3313

Zasiahnuté systémy

PowerSYSTEM Server vo verzii staršej ako 4.09.00.927
Substation Server 2021 vo verzii staršej ako 4.09.00.927

Následky

Eskalácia privilégií
Zneprístupnenie služby
Vykonanie škodlivého kódu
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame kontaktovať výrobcu za účelom vykonania aktualizácie 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.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-100-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitel MiCollab - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mitel vydala bezpečnostnú aktualizáciu na svoj produkt MiCollab, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2024-30159 a CVE-2024-30160 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom XSS (Cross Site Scripting) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.
Ostatné zraniteľnosti možno zneužiť na vykonanie SQL injekcie s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.4.2024

CVE

CVE-2024-30157, CVE-2024-30158, CVE-2024-30159, CVE-2024-30160

Zasiahnuté systémy

MiCollab vo verzii staršej ako 9.8

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin_24-0004-001-v1.pdf
https://www.mitel.com/-/media/mitel/file/pdf/support/security-advisories/security-bulletin_24-0005-001-v1.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	■ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Thesycon Software KG TUSBAudio MSI-based installers - bezpečnostná zraniteľnosť

Popis

Spoločnosť Thesycon Software vydala bezpečnostnú aktualizáciu na svoj produkt Thesycon Software KG TUSBAudio MSI-based installers, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-25376 nachádzajúca sa v komponente msiexec.exe spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených DLL súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.4.2024

CVE

CVE-2024-25376

Zasiahnuté systémy

Thesycon Software KG TUSBAudio MSI-based installers vo verzii staršej ako 5.68.0

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/287490

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

Identifikátor

Palo Alto Networks PAN-OS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Palo Alto Networks vydala bezpečnostné aktualizácie, ktoré opravujú viacero bezpečnostných zraniteľností v softvéri PAN-OS.
Najzávažnejšia zraniteľnosť s identifikátorom CVE-2024-3383 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej Cloud Identity Engine (CIE) požiadavky vykonať neoprávnené zmeny v systéme alebo spôsobiť zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.4.2024

CVE

CVE-2024-3383, CVE-2024-3385, CVE-2024-3382, CVE-2024-3384, CVE-2024-3386, CVE-2024-3387, CVE-2024-3388

Zasiahnuté systémy

PAN-OS

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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 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://security.paloaltonetworks.com/CVE-2024-3383
https://security.paloaltonetworks.com/CVE-2024-3385
https://security.paloaltonetworks.com/CVE-2024-3382
https://security.paloaltonetworks.com/CVE-2024-3384
https://security.paloaltonetworks.com/CVE-2024-3386
https://security.paloaltonetworks.com/CVE-2024-3387
https://security.paloaltonetworks.com/CVE-2024-3388

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

Identifikátor

Zauberzeug NiceGUI - bezpečnostná zraniteľnosť

Popis

Spoločnosť Zauberzeug vydala bezpečnostnú aktualizáciu na svoj produkt NiceGUI, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-32005 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

11.4.2024

CVE

CVE-2024-32005

Zasiahnuté systémy

Zauberzeug NiceGUI vo verzii staršej ako 1.4.21.

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://exchange.xforce.ibmcloud.com/vulnerabilities/287625
https://github.com/zauberzeug/nicegui/security/advisories/GHSA-mwc7-64wg-pgvj

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

Identifikátor

Tp-Link produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Tp-Link vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2023-49133 a CVE-2023-49134 sa nachádzajú v zariadeniach Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926 a Tp-Link N300 Wireless Access Point (EAP115 V4) v5.0.4 Build 20220216, spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov 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

9.4.2024

CVE

CVE-2023-49133, CVE-2023-49134, CVE-2023-49074, CVE-2023-48724, CVE-2023-49907, CVE-2023-49910, CVE-2023-49911, CVE-2023-49908, CVE-2023-49912, CVE-2023-49909, CVE-2023-49906, CVE-2023-49913

Zasiahnuté systémy

Tp-Link N300 Wireless Access Point (EAP115) v5.0.4 Build 20220216
Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926
Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926
Tp-Link N300 Wireless Access Point (EAP115) v5.0.4 Build 20220216
Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926
Tp-Link N300 Wireless Access Point (EAP115) v5.0.4 Build 20220216
Tp-Link AC1350 Wireless MU-MIMO Gigabit Access Point (EAP225 V3) v5.1.0 Build 20220926

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 na najnovšiu verziu firmvéru EAP115 V4 dostupnej na stránke výrobcu uvedenej 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://talosintelligence.com/vulnerability_reports/TALOS-2023-1862
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1861
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1864
https://talosintelligence.com/vulnerability_reports/TALOS-2023-1888
https://www.tp-link.com/us/support/download/eap115/v4/#Firmware%20https://www.tp-link.com/us/support/download/eap225/v3/#Firmware

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

Identifikátor

Pepperl+Fuchs SE ICE2 a ICE3 produkty - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o viacerých bezpečnostných zraniteľnostiach produktov ICE2 a ICE3.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2002-20001 a CVE-2022-40735 spočívajú v v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej sieťovej prevádzky spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na neoprávnené zmeny v systéme a neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

10.4.2024

CVE

CVE-2002-20001, CVE-2022-40735, CVE-2022-31629, CVE-2021-21707, CVE-2020-7070, CVE-2004-0230, CVE-2011-3389, CVE-1999-0524

Zasiahnuté systémy

ICE2-8IOL1-G65L-V1D vo verzii staršej ako (vrátane) 1.6.50
ICE2-8IOL-G65L-V1D vo verzii staršej ako (vrátane) 1.6.50
ICE2-8IOL-K45P-RJ45 vo verzii staršej ako (vrátane) 1.6.50
ICE2-8IOL-K45S-RJ45 vo verzii staršej ako (vrátane) 1.6.50
ICE3-8IOL1-G65L-V1D vo verzii staršej ako (vrátane) 1.6.50
ICE3-8IOL-G65L-V1D vo verzii staršej ako (vrátane) 1.6.50
ICE3-8IOL-G65L-V1D-Y vo verzii staršej ako (vrátane) 1.6.50
ICE3-8IOL-K45P-RJ45 vo verzii staršej ako (vrátane) 1.6.50
ICE3-8IOL-K45S-RJ45 vo verzii staršej ako (vrátane) 1.6.50

Následky

Zneprístupnenie služby
Neoprávnené zmeny v systéme
Neoprávnený prístup k citlivým údajom

Odporúčania

Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať. Detailné inštrukcie môžete nájsť na webovej adrese uvedenej v sekcii ZDROJE.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://cert.vde.com/en/advisories/VDE-2024-017/

BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 04. 2024 - 16. 04. 2024

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

Identifikátor

Juniper Networks Junos OS / Junos OS Evolved - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Juniper Networks vydala bezpečnostné aktualizácie na produkty Junos OS a Junos OS Evolved, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2024-30395, CVE-2024-30382 a CVE-2024-30397 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov v rámci komponentov zodpovedných za spracovanie protokolov BGP, RPD a IKE. Uvedené zraniteľnosti umožňujú vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.
Zneužitím ostatných bezpečnostných zraniteľností možno získať neoprávnený prístup k citlivým údajom a spôsobiť zneprístupnenie služby

Dátum prvého zverejnenia varovania

10.4.2024

CVE

CVE-2024-30397, CVE-2024-30395, CVE-2024-30382, CVE-2024-30406, CVE-2024-21618, CVE-2024-30405

Zasiahnuté systémy

Junos OS
Junos OS SRX 5000 Series with SPC2 with ALGs enabled
Junos OS Evolved

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom, je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-malformed-BGP-tunnel-encapsulation-attribute-will-lead-to-an-rpd-crash-CVE-2024-30395?language=en_US
https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Junos-OS-and-Junos-OS-Evolved-RPD-crash-when-CoS-based-forwarding-CBF-policy-is-configured-CVE-2024-30382?language=en_US
https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-An-invalid-certificate-causes-a-Denial-of-Service-in-the-Internet-Key-Exchange-IKE-process-CVE-2024-30397?language=en_US
https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-Evolved-ACX-Series-with-Paragon-Active-Assurance-Test-Agent-A-local-high-privileged-attacker-can-recover-other-administrators-credentials-CVE-2024-30406?language=en_US
https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-When-LLDP-is-enabled-and-a-malformed-LLDP-packet-is-received-l2cpd-crashes-CVE-2024-21618?language=en_US
https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-SRX-5000-Series-with-SPC2-Processing-of-specific-crafted-packets-when-ALG-is-enabled-causes-a-transit-traffic-Denial-of-Service-CVE-2024-30405?language=en_US

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

Rockwell Automation 5015-AENFTXT - bezpečnostná zraniteľnosť

Popis

Spoločnosť Rockwell Automation vydala bezpečnostnú aktualizáciu na svoj produkt 5015-AENFTXT, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2424 spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených PTP paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

11.4.2024

CVE

CVE-2024-2424

Zasiahnuté systémy

5015-AENFTXT vo verzii staršej ako v2.12.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
SK-CERT administrátorom odporúča venovať osobitnú pozornosť aktualizácii firmvéru, nie len aplikačnému softvéru.
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.
Pre dočasnú mitigáciu odporúčame postupovať podľa pokynov výrobcu uvedených na webovej adrese: https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight

Zdroje

https://www.rockwellautomation.com/en-us/support/advisory.SD1667.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/287443

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

Identifikátor

Spring by VMware Tanzu Spring Framework - bezpečnostná zraniteľnosť

Popis

Spoločnosť Spring by VMware Tanzu vydala bezpečnostnú aktualizáciu svojho produktu Spring Framework, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-22262 nachádzajúca sa v komponente UriComponentsBuilder spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom open redirect alebo server-side request forgery (SSRF) útoku vykonať neoprávnené zmeny v systéme. Zneužitie zraniteľnosti vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

11.4.2024

CVE

CVE-2024-22262

Zasiahnuté systémy

Spring Framework vo verzii staršej ako 6.1.6, 6.0.19 a 5.3.34

Následky

Neoprávnená zmena v systéme

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://spring.io/security/cve-2024-22262
https://exchange.xforce.ibmcloud.com/vulnerabilities/287586

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