BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 04. 2024 - 09. 04. 2024

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
1.	Google Chrome - bezpečnostné zraniteľnosti	Kritická	9.8
2.	Modal Popup Box WP plugin - bezpečnostná zraniteľnosť	Vysoká	8.8
3.	PLANEX COMMUNICATIONS MZK-MF300N - bezpečnostné zraniteľnosti	Vysoká	8.8
4.	Hewlett Packard Enterprise produkty - viacero bezpečnostných zraniteľností	Vysoká	8.8
5.	Pluginy redakčného systému WordPress - viacero bezpečnostných zraniteľností	Vysoká	8.8
6.	SAP produkty - viacero bezpečnostných zraniteľností	Vysoká	8.8
7.	X.Org X server - viacero bezpečnostných zraniteľnost	Vysoká	7.8
8.	Yubico YubiKey Manager GUI - bezpečnostná zraniteľnosť	Vysoká	7.7
9.	Cisco Nexus Dashboard - tri bezpečnostné zraniteľnosti	Vysoká	7.5
10.	Tempesta Technologies Tempesta FW - bezpečnostná zraniteľnosť	Vysoká	7.5
11.	Envoy Proxy Envoy - bezpečnostná zraniteľnosť	Vysoká	7.5
12.	Apache NimBLE - bezpečnostná zraniteľnosť	Vysoká	7.5
13.	ABB S+ produkty - bezpečnostná zraniteľnosť	Vysoká	7.5
14.	Apache Pulsar - bezpečnostná zraniteľnosť	Vysoká	7.4
15.	Sourcecodester Online Library System - bezpečnostná zraniteľnosť	Vysoká	7.3

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 03. 04. 2024 - 09. 04. 2024

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☐ **Vysoká**	■ **Kritická**	**CVSS skóre: 9.8**
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Google Chrome - bezpečnostné zraniteľnosti

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj produkt Google Chrome, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšie zraniteľnosti s označením CVE-2024-3158 a CVE-2024-3159 sa nachádzajú v komponentoch V8 a Bookmarks a vzdialený neautentifikovaný útočník by ich prostredníctvom podvrhnutia špeciálne vytvoreného webového obsahu mohol zneužiť na vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Poslednú zraniteľnosť možno zneužiť na obídenie bezpečnostných prvkov.

Dátum prvého zverejnenia varovania

2.4.2024

CVE

CVE-2024-3156, CVE-2024-3158, CVE-2024-3159

Zasiahnuté systémy

Google Chrome pre Android vo verzii staršej ako 123.0.6312.99
Google Chrome Desktop pre Windows & Mac vo verzii staršej ako 123.0.6312.105/106/107
Google Chrome Desktop pre Linux vo verzii staršej ako 123.0.6312.105

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Obídenie bezpečnostných prvkov

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne 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://chromereleases.googleblog.com/2024/04/chrome-for-android-update.html
https://chromereleases.googleblog.com/2024/04/stable-channel-update-for-desktop.html
https://www.tenable.com/cve/CVE-2024-3158
https://www.tenable.com/cve/CVE-2024-3159
https://www.tenable.com/cve/CVE-2024-3156

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

Modal Popup Box WP plugin - bezpečnostná zraniteľnosť

Popis

Vývojári WordPress pluginu Modal Popup Box vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2008 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

3.4.2024

CVE

CVE-2024-2008

Zasiahnuté systémy

Modal Popup Box vo verzii staršej ako 1.5.3

Následky

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

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/modal-popup-box/modal-popup-box-popup-builder-show-offers-and-news-in-popup-152-authenticated-contributor-php-object-injection-in-awl-modal-popup-box-shortcode

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

Identifikátor

PLANEX COMMUNICATIONS MZK-MF300N - bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o dvoch bezpečnostných zraniteľnostiach smerovaču MZK-MF300N od spoločnosti PLANEX COMMUNICATIONS.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-30220 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Bezpečnostnú zraniteľnosť s identifikátorom CVE-2024-30219 možno zneužiť na neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

4.4.2024

CVE

CVE-2024-30219, CVE-2024-30220

Zasiahnuté systémy

Smerovače PLANEX COMMUNICATIONS MZK-MF300N vo všetkých verziách (ukončená podpora)

Následky

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

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
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://jvn.jp/en/vu/JVNVU91975826/index.html

BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 04. 2024 - 09. 04. 2024

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

Identifikátor

Hewlett Packard Enterprise produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostné aktualizácie na svoje portfólio serverov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti s identifikátormi CVE-2023-45235, CVE-2023-45234 a CVE-2023-45230 sa nachádzajú v serveroch rady HPE ProLiant DL/ML/SY/RL/XL/Edgeline, spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov komponentu EDK2's Network Package a umožňujú neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente 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

2.4.2024

CVE

CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2021-38575

Zasiahnuté systémy

HPE ProLiant DL110 Gen11 vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant DL320 Gen11 Server vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant DL360 Gen11 Server vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant DL380 Gen11 Server vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant DL380a Gen11 vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant DL560 Gen11 vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant ML110 Gen11 vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant ML350 Gen11 Server vo verzii staršej ako v2.16_03-01-2024
HPE Alletra 4110 vo verzii staršej ako v2.16_03-01-2024
HPE Alletra 4120 vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant DL110 Gen10 Plus Telco server vo verzii staršej ako v2.00_02-22-2024
HPE ProLiant DL360 Gen10 Plus server vo verzii staršej ako v2.00_03-06-2024
HPE ProLiant DL380 Gen10 Plus server vo verzii staršej ako v2.00_03-06-2024
HPE ProLiant DL160 Gen10 Server vo verzii staršej ako v3.10_02-22-2024
HPE ProLiant DL180 Gen10 Server vo verzii staršej ako v3.10_02-22-2024
HPE ProLiant DL360 Gen10 Server vo verzii staršej ako v3.10_02-22-2024
HPE ProLiant DL380 Gen10 Server vo verzii staršej ako v3.10_02-22-2024
HPE ProLiant DL560 Gen10 Server vo verzii staršej ako v3.10_02-22-2024
HPE ProLiant ML110 Gen10 Server vo verzii staršej ako v3.10_02-22-2024
HPE ProLiant ML350 Gen10 Server vo verzii staršej ako v3.10_02-22-2024
HPE Synergy 480 Gen11 Compute Module vo verzii staršej ako v2.16_03-01-2024
HPE Synergy 480 Gen10 Plus Compute Module vo verzii staršej ako v2.00_02-22-2024
HPE ProLiant BL460c Gen10 Server Blade vo verzii staršej ako v3.10_02-22-2024
HPE Synergy 480 Gen10 Compute Module vo verzii staršej ako v3.10_02-22-2024
HPE Synergy 660 Gen10 Compute Module vo verzii staršej ako v3.10_02-22-2024
HPE Apollo 4200 Gen10 Plus System vo verzii staršej ako v2.00_02-22-2024
HPE ProLiant XL220n Gen10 Plus Server vo verzii staršej ako v2.00_02-22-2024
HPE ProLiant XL290n Gen10 Plus Server vo verzii staršej ako v2.00_02-22-2024
HPE Apollo 2000 Gen10 Plus System vo verzii staršej ako v2.00_02-22-2024
HPE Apollo 2000 System vo verzii staršej ako v3.10_02-22-2024

HPE ProLiant e910 Server Blade vo verzii staršej ako v3.10_02-22-2024
HPE ProLiant e910t Server Blade vo verzii staršej ako v3.10_02-22-2024
HPE Edgeline e920 Server Blade vo verzii staršej ako v2.00_02-22-2024
HPE Edgeline e920d Server Blade vo verzii staršej ako v2.00_02-22-2024
HPE Edgeline e920t Server Blade vo verzii staršej ako v2.00_02-22-2024
HPE Compute Edge Server e930t vo verzii staršej ako v2.16_03-01-2024
HPE ProLiant XL225n Gen10 Plus 1U Node vo verzii staršej ako v3.00_01-26-2024
HPE ProLiant RL300 Gen11 vo verzii staršej ako v1.60_03-07-2024

Následky

Neoprávnený prístup do systému
Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom
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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04593en_us
https://nvd.nist.gov/vuln/detail/CVE-2023-45235
https://nvd.nist.gov/vuln/detail/CVE-2023-45234
https://nvd.nist.gov/vuln/detail/CVE-2023-45230

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 ElementsKit Elementor addons, CRM Perks Forms, Element Pack Elementor Addons a WP ERP pluginov pre WordPress vydali bezpečnosté aktualizácie svojich produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2047 sa nachádza v ElementsKit Elementor addons WP plugine, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvorených súborov 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

29.3.2024

CVE

CVE-2024-2047, CVE-2024-30499, CVE-2024-30496, CVE-2024-0608

Zasiahnuté systémy

ElementsKit Elementor addons vo verzii staršej ako 3.0.7
CRM Perks Forms vo verzii staršej ako 1.1.5
Element Pack Elementor Addons vo verzii staršej ako 5.5.4
WP ERP vo verzii staršej ako 1.12.9 (vrátane)

Následky

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

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetné pluginy v zraniteľnej verzii. V prípade, že áno, bezodkladne zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Pre WP ERP plugin a jeho uvedenú bezpečnostnú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame do vydania záplat pluginy v zraniteľných verziách dočasne deaktivovať alebo odinštalovať a vykonať kontrolu integrity 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/elementskit-lite/elementskit-elementor-addons-306-authenticated-contributor-local-file-inclusion-in-render-raw
https://patchstack.com/database/vulnerability/crm-perks-forms/wordpress-crm-perks-forms-plugin-1-1-4-sql-injection-vulnerability
https://patchstack.com/database/vulnerability/bdthemes-element-pack-lite/wordpress-element-pack-lite-plugin-5-5-3-sql-injection-vulnerability
https://patchstack.com/database/vulnerability/erp/wordpress-wp-erp-plugin-1-12-9-authenticated-subscriber-sql-injection-vulnerability

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

Identifikátor

SAP produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť SAP vydala bezpečnostné aktualizácie na svoje porfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-27899 nachádzajúca sa v produkte SAP NetWeaver AS Java User Management Engine spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Ostatné bezpečnostné zraniteľnosti možno zneužiť na vykonanie škodlivého kódu, neoprávnený prístup k citlivým údajom, neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

9.4.2024

CVE

CVE-2024-27899, CVE-2024-25646, CVE-2024-27901, CVE-2024-30218, CVE-2024-28167, CVE-2022-29613, CVE-2023-40306, CVE-2024-27898, CVE-2024-30214, CVE-2024-30215, CVE-2024-30216, CVE-2024-30217

Zasiahnuté systémy

SAP NetWeaver AS Java User Management Engine bez aplikovanej bezpečnostnej záplaty vo verziách SERVERCORE 7.50, J2EE-APPS 7.50 a UMEADMIN 7.50
SAP BusinessObjects Web Intelligence bez aplikovanej bezpečnostnej záplaty vo verziách 4.2 a 4.3
SAP Asset Accounting bez aplikovanej bezpečnostnej záplaty vo verziách SAP_APPL 600, SAP_FIN617, SAP_FIN 618 a SAP_FIN700
SAP Edge Integration Cell vo verzii staršej ako 8.13.5
SAP NetWeaver AS ABAP a ABAP Platform bez aplikovanej bezpečnostnej záplaty vo verziách KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL 7.53, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54 a KERNEL 7.93
SAP Group Reporting Data Collection (Enter Package Data) bez aplikovanej bezpečnostnej záplaty vo verziách S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, SAP_GRDC_CLOUD 1.0.0
SAP Employee Self Service (Fiori My Leave Request) bez aplikovanej bezpečnostnej záplaty vo verzii 605
SAP S/4HANA (Manage Catalog Items and Cross-Catalog search) bez aplikovanej bezpečnostnej záplaty vo verziách S4CORE 103, S4CORE 104, S4CORE 105 a S4CORE 106
SAP NetWeaver bez aplikovanej bezpečnostnej záplaty vo verzii 7.50
SAP Business Connector bez aplikovanej bezpečnostnej záplaty vo verzii 4.8
SAP S/4 HANA (Cash Management) bez aplikovanej bezpečnostnej záplaty vo verziách S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108

Následky

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

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://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2024.html https://nvd.nist.gov/vuln/detail/CVE-2024-27899

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

Identifikátor

X.Org X server - viacero bezpečnostných zraniteľnost

Popis

Vývojári open-source implementácie X Window System X.ORG vydali bezpečnostnú aktualizáciu svojich produktov X Server a Xwayland, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostné zraniteľnosti s identifikátormi CVE-2024-31083, CVE-2024-31082, CVE-2024-31081 a CVE-2024-31080 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom znovupoužitia uvoľnenej pamäte alebo prostredníctvom pretečenia zásobníka vykonanie škodlivého kódu s následkom úplného narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

3.4.2024

CVE

CVE-2024-31083, CVE-2024-31082, CVE-2024-31081, CVE-2024-31080

Zasiahnuté systémy

X server vo verzii staršej ako 21.1.12
Xwayland vo verzii staršej ako 23.2.5

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/286915
https://exchange.xforce.ibmcloud.com/vulnerabilities/286914
https://exchange.xforce.ibmcloud.com/vulnerabilities/286913
https://exchange.xforce.ibmcloud.com/vulnerabilities/286912

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

Identifikátor

Yubico YubiKey Manager GUI - bezpečnostná zraniteľnosť

Popis

Spoločnosť Yubico vydala bezpečnostnú aktualizáciu na svoj produkt YubiKey Manager, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť sa nachádza v komponente YubiKey Manager GUI (ykman-gui), spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami administrátora eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Zneužitie zraniteľnosti je možné len na systémoch s operačným systémom WINDOWS a vyžaduje interakciu zo strany používateľa.

Dátum prvého zverejnenia varovania

4.4.2024

CVE

Zasiahnuté systémy

YubiKey Manager GUI vo verzii staršej ako 1.2.6 na systémoch s operačným systémom WINDOWS

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.

Zdroje

https://www.yubico.com/support/security-advisories/ysa-2024-01/
https://exchange.xforce.ibmcloud.com/vulnerabilities/286948

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

Identifikátor

Cisco Nexus Dashboard - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostné aktualizácie na produkty Cisco Nexus Dashboard, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s identifikátorom CVE-2024-20348 sa nachádza v produkte Cisco Nexus Dashboard Fabric Controller (NDFC), spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.
Zneužitím ostatných bezpečnostných zraniteľností možno vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

3.4.2024

CVE

CVE-2024-20281, CVE-2024-20348, CVE-2024-20283

Zasiahnuté systémy

Cisco NDFC
Cisco Nexus Dashboard
Cisco NDI
Cisco NDO

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-dir-trav-SSn3AYDw
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfccsrf-TEmZEfJ9
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndidv-LmXdvAf2

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

Identifikátor

Tempesta Technologies Tempesta FW - bezpečnostná zraniteľnosť

Popis

Vývojári open source aplikácie Tempesta FW vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-2758 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

4.4.2024

CVE

CVE-2024-2758

Zasiahnuté systémy

Tempesta FW vo verzii staršej ako 0.7.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/286957
https://github.com/tempesta-tech/tempesta/security/advisories/GHSA-3xwj-5ch3-q9p4

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

Identifikátor

Envoy Proxy Envoy - bezpečnostná zraniteľnosť

Popis

Vývojári open source proxy Envoy Proxy Envoy vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje jednu bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-27919 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

3.4.2024

CVE

CVE-2024-27919

Zasiahnuté systémy

Envoy Proxy Envoy vo verzii staršej ako 1.29.2

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/286956
https://github.com/envoyproxy/envoy/security/advisories/GHSA-gghf-vfxp-799r

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

Identifikátor

Apache NimBLE - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj open-source Bluetooth 5.0 stacku Apache nimBLE, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-24746 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonaním špeciálnych GATT operácií spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

4.4.2024

CVE

CVE-2024-24746

Zasiahnuté systémy

Apache NimBLE vo verzii staršej ako 1.7.0

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/287158

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

ABB S+ produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť ABB vydala bezpečnostné aktualizácie na produkty S+ Operations, S+ Engineering a S+ Analyst, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-0335 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov komponentu Virtual PNI a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených VPNI paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

26.3.2024

CVE

CVE-2024-0335

Zasiahnuté systémy

S+ Operations vo verzii staršej ako (vrátane) 3.3 SP1 RU4 (bezpečnostná záplata s označením 3.3 SP1 RU5 má plánované vydanie Q3 2024)
S+ Operations vo verzii staršej ako (vrátane) 2.1 SP2 RU3 bezpečnostná záplata s označením 3.3 SP1 RU5 má plánované vydanie Q3 2024)
S+ Operations vo verzii staršej ako (vrátane) 2.0 SP6 TC6 bezpečnostná záplata s označením 3.3 SP1 RU5 má plánované vydanie Q3 2024)
S+ Engineering vo verzii staršej ako 2.4
S+ Analyst with the Fast Data Logger vo verzii staršej ako (vrátane) 7.2.0.2 (bezpečnostná záplata s označením 7.3 má plánované vydanie Q2 2024)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať. Detailné inštrukcie môžete nájsť na webovej adrese uvedenej v sekcii ZDROJE.
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://library.e.abb.com/public/2a16709fe6854d5b8849b548cda89030/7PAA002536_A_en_Cyber%20Security%20Advisory_Virtual_PNI.pdf?x-sign=qDeYPaXJ/tCTDr806TVlc2QkakR/0iFCbbQ4le6FHrWcE82fuA4rw7BTrSAyQxDC

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

Identifikátor

Apache Pulsar - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apache vydala bezpečnostnú aktualizáciu na svoj produkt Apache Pulsar, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-29834 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

2.4.2024

CVE

CVE-2024-29834

Zasiahnuté systémy

Apache Pulsar vo verzii 2.7.1 až 2.10.6
Apache Pulsar vo verzii 2.11.0 až 2.11.4
Apache Pulsar vo verzii 3.0.0 až do verzie staršej ako 3.0.4
Apache Pulsar vo verzii 3.1.0 až 3.1.3
Apache Pulsar vo verzii 3.2.0 až do verzie staršej ako 3.2.2

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

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

Zdroje

https://pulsar.apache.org/security/CVE-2024-29834/
https://exchange.xforce.ibmcloud.com/vulnerabilities/286806

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:** 7.3
Klasifikácia	■ **Neutajované / TLP:CLEAR**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Sourcecodester Online Library System - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Sourcecodester Online Library System.
Bezpečnostná zraniteľnosť s identifikátorom CVE-2024-3363 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom SQL injekcie vykonať škodlivý kód a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme alebo spôsobiť zneprístupnenie služby.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

4.4.2024

CVE

CVE-2024-3363

Zasiahnuté systémy

SourceCodester Online Library System vo verzii staršej ako 1.0 (vrátane)

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.
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/287248
https://vuldb.com/?submit.310429

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