BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 06. 2023 - 13. 06. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	GitLab - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Mozilla Firefox - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	mailcow - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	TI WooCommerce Wishlist - bezpečnostná zraniteľnosť	Vysoká	**8.8**
06.	Kali Forms pre WP - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	Thunderbird - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
08.	SAP produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
09.	Fortinet produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
10.	Western Digital MyCloud zariadenia - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
11.	Qualcomm Chipsety - viacero bezpečnostných zraniteľností	Vysoká	**8.4**
12.	Sensormatic Electronics Illustra Pro Gen 4 - bezpečnostná zraniteľnosť	Vysoká	**8.3**
13.	CNCSoft-B DOPSoft - dve bezpečnostné zraniteľnosti	Vysoká	**7.8**
14.	Linux Kernel - bezpečnostná zraniteľnosť	Vysoká	**7.8**
15.	Fuji Electric V-Server a TELLUS - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
16.	Ashlar-Vellum Cobalt - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
17.	Trend Micro Apex One - tri bezpečnostné zraniteľnosti	Vysoká	**7.8**
18.	MELSEC iQ-R - viacero bezpečnostných zraniteľností	Vysoká	**7.5**
19.	OpenProject - bezpečnostná zraniteľnosť	Vysoká	**7.5**
20.	Brocade produkty - bezpečnostná zraniteľnosť	Vysoká	**7.5**
21.	Grafana - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
22.	Advantech WebAccess/SCADA - tri bezpečnostné zraniteľnosti	Vysoká	**7.2**
23.	ZTE MF286R router - zero-day bezpečnostná zraniteľnosť	Stredná	**6.8**

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
Naša značka:
01794/2022/SK-CERT-1182

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

Identifikátor

GitLab - viacero bezpečnostných zraniteľností

Popis

Vývojári platformy GitLab vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi prostredníctvom stored cross-site scripting (XSS) útoku vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

05.06.2023

CVE

CVE-2023-0121, CVE-2023-0508, CVE-2023-0921, CVE-2023-1204, CVE-2023-1825, CVE-2023-2001, CVE-2023-2013, CVE-2023-2015, CVE-2023-2132, CVE-2023-2198, CVE-2023-2199, CVE-2023-2442, CVE-2023-2485, CVE-2023-2589

Zasiahnuté systémy

GitLab Community Edition vo verzii staršej ako 16.0.2, 15.11.7 a 15.10.8
GitLab Enterprise Edition vo verzii staršej ako 16.0.2, 15.11.7 a 15.10.8

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://about.gitlab.com/releases/2023/06/05/security-release-gitlab-16-0-2-released/

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

Identifikátor

Google Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť 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.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

05.06.2023

CVE

CVE-2023-3079

Zasiahnuté systémy

Desktop release (Windows: 114.0.5735.100/.91, Mac & Linux: 114.0.5735.106)
Chrome 114 (114.0.5735.60/.61) for Android

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/
https://www.bleepingcomputer.com/news/security/google-fixes-new-chrome-zero-day-flaw-with-exploit-in-the-wild/

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

Identifikátor

Mozilla Firefox - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla vydala bezpečnostné aktualizácie na prehliadače Firefox a Firefox ESR, ktoré opravujú viacero bezpečnostných zraniteľností.
Bezpečnostná zraniteľnosť 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.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2023-34414, CVE-2023-34415, CVE-2023-34416, CVE-2023-34417

Zasiahnuté systémy

Firefox ESR vo verzii staršej ako 102.12
Firefox vo verzii staršej ako 114

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 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://www.mozilla.org/en-US/security/advisories/mfsa2023-20/
https://exchange.xforce.ibmcloud.com/vulnerabilities/257264

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

Identifikátor

mailcow - bezpečnostná zraniteľnosť

Popis

Vývojári open source mailserveru mailcow vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zasielania špeciálne vytvorených hesiel získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.06.2023

CVE

CVE-2023-34108

Zasiahnuté systémy

mailcow vo verzii staršej ako 2023-05a

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

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://github.com/mailcow/mailcow-dockerized/security/advisories/GHSA-mhh4-qchc-pv22
https://exchange.xforce.ibmcloud.com/vulnerabilities/257584

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

Identifikátor

TI WooCommerce Wishlist - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu TI WooCommerce Wishlist pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

07.06.2023

CVE

CVE-2020-36725

Zasiahnuté systémy

TI WooCommerce Wishlist plugin pre WordPress vo verzii staršej ako 1.21.12

Následky

Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, 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 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/257534

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

Identifikátor

Kali Forms pre WP - bezpečnostná zraniteľnosť

Popis

Vývojári pluginu Kali Forms pre WordPress vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom CSRF (Cross Site Request Forgery) útoku spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.
Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

07.06.2023

CVE

CVE-2020-36717

Zasiahnuté systémy

Kali Forms plugin pre WordPress vo verzii staršej ako 2.1.2

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky a aplikácie založené na redakčnom systéme WordPress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu redakčného systému a všetkých používaných pluginov na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/257542

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

Identifikátor

Thunderbird - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu na svoj produkt Thunderbird, ktorá opravuje dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť 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.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2023-34414, CVE-2023-34416

Zasiahnuté systémy

Mozilla Thunderbird vo verzii staršej ako 102.12

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.mozilla.org/en-US/security/advisories/mfsa2023-21/
https://exchange.xforce.ibmcloud.com/vulnerabilities/257261

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 portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.06.2023

CVE

CVE-2021-42063, CVE-2022-22542, CVE-2023-2827, CVE-2023-30742, CVE-2023-30743, CVE-2023-31406, CVE-2023-32114, CVE-2023-32115, CVE-2023-33984, CVE-2023-33985, CVE-2023-33986, CVE-2023-33991

Zasiahnuté systémy

SAP NetWeaver
SAP Knowledge Warehouse
SAP UI5 Variant Management
SAP Plant Connectivity
SAPUI5
SAP S/4HANA (Supplier Factsheet and Enterprise Search for
Business Partner, Supplier and Customer)
SAP NetWeaver Enterprise Portal
SAP CRM ABAP
SAP CRM (WebClient UI)
SAP BusinessObjects Business Intelligence Platform
Master Data Synchronization (MDS COMPARE TOOL)
SAP NetWeaver (Change and Transport System)

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti ZDROJE

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://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

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

Identifikátor

Fortinet produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Fortinet vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

13.06.2023

CVE

CVE-2022-33877, CVE-2022-39946, CVE-2022-41327, CVE-2022-42474, CVE-2022-42478, CVE-2022-43949, CVE-2022-43953, CVE-2023-22633, CVE-2023-22639, CVE-2023-25609, CVE-2023-26204, CVE-2023-26207, CVE-2023-26210, CVE-2023-28000, CVE-2023-29175, CVE-2023-29178, CVE-2023-29179, CVE-2023-29180, CVE-2023-29181, CVE-2023-33305

Zasiahnuté systémy

FortiNAC-F vo verzii staršej ako 7.2.1
FortiNAC vo verzii staršej ako 9.4.2
FortiNAC vo verzii staršej ako 9.2.7
FortiNAC vo verzii staršej ako 9.1.9
FortiNAC-F vo verzii staršej ako 7.2.0
FortiNAC vo verzii staršej ako 9.4.3
FortiNAC vo verzii staršej ako 9.2.8
FortiAnalyzer vo verzii staršej ako 7.2.2
FortiAnalyzer vo verzii staršej ako 7.0.7
FortiAnalyzer vo verzii staršej ako 6.4.12
FortiManager vo verzii staršej ako 7.2.2
FortiManager vo verzii staršej ako 7.0.7
FortiManager vo verzii staršej ako 6.4.12
FortiClientWindows vo verzii staršej ako 7.0.7
FortiClientWindows vo verzii staršej ako 6.4.9
FortiConverter vo verzii staršej ako 7.0.1
FortiConverter vo verzii staršej ako 6.2.2
FortiADC vo verzii staršej ako 7.1.1
FortiADC vo verzii staršej ako 7.0.4
FortiADC vo verzii staršej ako 6.2.5
FortiADC vo verzii staršej ako 7.2.1
FortiADC vo verzii staršej ako 7.1.3
FortiADCManager vo verzii staršej ako 7.2.0

FortiADCManager vo verzii staršej ako 7.1.1
FortiADCManager vo verzii staršej ako 7.0.1
FortiSIEM vo verzii staršej ako 7.0.0
FortiSIEM vo verzii staršej ako 6.7.2
FortiSIEM vo verzii staršej ako 7.0.0
FortiSIEM vo verzii staršej ako 6.7.1
FortiOS vo verzii staršej ako 7.2.5
FortiOS vo verzii staršej ako 7.0.9
FortiProxy vo verzii staršej ako 7.2.2
FortiProxy vo verzii staršej ako 7.0.8
FortiPAM vo verzii staršej ako 1.0.0
FortiWeb vo verzii staršej ako 7.2.2
FortiWeb vo verzii staršej ako 7.0.7
FortiOS vo verzii staršej ako 7.4.0
FortiOS vo verzii staršej ako 7.0.11
FortiProxy vo verzii staršej ako 7.2.4
FortiProxy vo verzii staršej ako 7.0.10
FortiOS vo verzii staršej ako 7.2.4
FortiOS vo verzii staršej ako 7.0.10
FortiOS vo verzii staršej ako 6.4.13
FortiSwitchManager vo verzii staršej ako 7.2.2
FortiSwitchManager vo verzii staršej ako 7.0.2
FortiProxy vo verzii staršej ako 2.0.12
FortiOS vo verzii staršej ako 7.0.12
FortiOS vo verzii staršej ako 6.2.15
FortiOS vo verzii staršej ako 6.0.17
FortiProxy vo verzii staršej ako 7.2.2
FortiProxy vo verzii staršej ako 7.2.3
FortiProxy vo verzii staršej ako 7.0.9
FortiOS vo verzii staršej ako 7.2.1
FortiOS vo verzii staršej ako 6.4.13

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
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/257789
https://www.fortiguard.com/psirt/FG-IR-23-095
https://www.fortiguard.com/psirt/FG-IR-22-463
https://www.fortiguard.com/psirt/FG-IR-22-468
https://www.fortiguard.com/psirt/FG-IR-22-494
https://www.fortiguard.com/psirt/FG-IR-22-455
https://www.fortiguard.com/psirt/FG-IR-23-119
https://www.fortiguard.com/psirt/FG-IR-23-111
https://www.fortiguard.com/psirt/FG-IR-23-125
https://www.fortiguard.com/psirt/FG-IR-22-393
https://www.fortiguard.com/psirt/FG-IR-22-375
https://www.fortiguard.com/psirt/FG-IR-22-380
https://www.fortiguard.com/psirt/FG-IR-22-258
https://www.fortiguard.com/psirt/FG-IR-21-141
https://www.fortiguard.com/psirt/FG-IR-22-259
https://www.fortiguard.com/psirt/FG-IR-23-076
https://www.fortiguard.com/psirt/FG-IR-23-107
https://www.fortiguard.com/psirt/FG-IR-22-229
https://www.fortiguard.com/psirt/FG-IR-22-493
https://www.fortiguard.com/psirt/FG-IR-22-332
https://www.fortiguard.com/psirt/FG-IR-22-521

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

Identifikátor

Western Digital MyCloud zariadenia - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Western Digital vydala bezpečnostnú aktualizáciu na svoje cloudové úložiská série MyCloud, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.06.2023

CVE

CVE-2022-29840, CVE-2022-29841, CVE-2022-29842, CVE-2022-36326, CVE-2022-36328, CVE-2022-36331

Zasiahnuté systémy

My Cloud OS 5 Firmware vo verzii staršej ako 5.26.119

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
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.zerodayinitiative.com/advisories/ZDI-23-852/
https://www.zerodayinitiative.com/advisories/ZDI-23-851/
https://www.zerodayinitiative.com/advisories/ZDI-23-850/
https://www.zerodayinitiative.com/advisories/ZDI-23-849/
https://www.zerodayinitiative.com/advisories/ZDI-23-848/
https://www.zerodayinitiative.com/advisories/ZDI-23-847/
https://www.zerodayinitiative.com/advisories/ZDI-23-846/

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

Identifikátor

Qualcomm Chipsety - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Qualcomm vydala bezpečnostné aktualizácie na svoje portfólio chipsetov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

05.06.2023

CVE

CVE-2022-22060, CVE-2022-22076, CVE-2022-33224, CVE-2022-33226, CVE-2022-33227, CVE-2022-33230, CVE-2022-33240, CVE-2022-33251, CVE-2022-33263, CVE-2022-33264, CVE-2022-33267, CVE-2022-33303, CVE-2022-33307, CVE-2022-40507, CVE-2022-40521, CVE-2022-40522, CVE-2022-40523, CVE-2022-40525, CVE-2022-40529, CVE-2022-40533, CVE-2022-40536, CVE-2022-40538, CVE-2023-21628, CVE-2023-21632, CVE-2023-21656, CVE-2023-21657, CVE-2023-21658, CVE-2023-21659, CVE-2023-21660, CVE-2023-21661, CVE-2023-21669, CVE-2023-21670

Zasiahnuté systémy

Qualcomm Chipsety

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti 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://docs.qualcomm.com/product/publicresources/securitybulletin/june-2023-bulletin.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/257289

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

Identifikátor

Sensormatic Electronics Illustra Pro Gen 4 - bezpečnostná zraniteľnosť

Popis

Spoločnosť Sensormatic Electronics vydala bezpečnostnú aktualizáciu na svoj produkt Illustra Pro Gen 4, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup k prihlasovacím údajom a následne získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

08.06.2023

CVE

CVE-2023-0954

Zasiahnuté systémy

Illustra Pro Gen 4 Dome vo verzii staršej ako 6.00.00
Illustra Pro Gen 4 PTZ vo verzii staršej ako 6.00.00

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

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.cisa.gov/news-events/ics-advisories/icsa-23-159-02

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

Identifikátor

CNCSoft-B DOPSoft - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt CNCSoft-B DOPSoft, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2023-24014, CVE-2023-25177

Zasiahnuté systémy

CNCSoft-B DOPSoft vo verzii staršej ako v4.0.0.82

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://www.cisa.gov/news-events/ics-advisories/icsa-23-157-01

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

Identifikátor

Linux Kernel - bezpečnostná zraniteľnosť

Popis

Vývojári jadra operačného systému Linux vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.
Zraniteľnosť zatiaľ nemá pridelený identifikátor CVE.

Dátum prvého zverejnenia varovania

07.06.2023

CVE

-

Zasiahnuté systémy

Linux Kernel vo verzii pred commitom 4d56304e5827c8cc8cc18c75343d283af7c4825c

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

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://seclists.org/oss-sec/2023/q2/213
https://exchange.xforce.ibmcloud.com/vulnerabilities/257458

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

Identifikátor

Fuji Electric V-Server a TELLUS - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Fuji Electric vydala bezpečnostné aktualizácie na svoje portfólio produktov V-Server a TELLUS, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.06.2023

CVE

CVE-2023-31239, CVE-2023-32201, CVE-2023-32270, CVE-2023-32273, CVE-2023-32276, CVE-2023-32288, CVE-2023-32538, CVE-2023-32542

Zasiahnuté systémy

V-Server vo verzii staršej ako v4.0.15.0 (vrátane)
V-Server Lite vo verzii staršej ako v4.0.15.0 (vrátane)
TELLUS vo verzii staršej ako v4.0.15.0 (vrátane)
TELLUS Lite vo verzii staršej ako v4.0.15.0 (vrátane)

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

http://jvn.jp/en/vu/JVNVU98818508/index.html

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

Spoločnosť Ashlar-Vellum vydala bezpečnostnú aktualizáciu na svoj produkt Cobalt, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov alebo webstránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

08.06.2023

CVE

CVE-2023-34286, CVE-2023-34287, CVE-2023-34288, CVE-2023-34289, CVE-2023-34290, CVE-2023-34291, CVE-2023-34292, CVE-2023-34293

Zasiahnuté systémy

Cobalt vo verzii staršej ako 12.0.1204.54

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.zerodayinitiative.com/advisories/ZDI-23-824/
https://www.zerodayinitiative.com/advisories/ZDI-23-825/
https://www.zerodayinitiative.com/advisories/ZDI-23-826/
https://www.zerodayinitiative.com/advisories/ZDI-23-827/
https://www.zerodayinitiative.com/advisories/ZDI-23-828/
https://www.zerodayinitiative.com/advisories/ZDI-23-829/
https://www.zerodayinitiative.com/advisories/ZDI-23-830/
https://www.zerodayinitiative.com/advisories/ZDI-23-831/

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

Identifikátor

Trend Micro Apex One - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Trend Micro vydala bezpečnostnú aktualizáciu na svoj produkt Apex One, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2023-34144, CVE-2023-34146, CVE-2023-34148

Zasiahnuté systémy

Apex One vo verzii staršej ako SP1 CP B12033
Apex One as a Service vo verzii staršej ako Build 202305, Security Agent version: 14.0.12518

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého 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://success.trendmicro.com/dcx/s/solution/000293322?language=en_US
https://www.zerodayinitiative.com/advisories/ZDI-23-834/

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

Identifikátor

MELSEC iQ-R - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu MELSEC iQ-R Series/iQ-F Series EtherNet/IP Modules a konfiguračného nástroja EtherNet/IP.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie v rámci FTP modulu a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup do systému a následne vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2023-2060, CVE-2023-2061, CVE-2023-2062, CVE-2023-2063

Zasiahnuté systémy

MELSEC iQ-R Series/iQ-F Series vo všetkých verziách
EtherNet/IP Modules vo všetkých verziách
EtherNet/IP Configuration tool vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému
Neoprávnená zmena v systéme

Odporúčania

Odporúčame postupovať podľa pokynov výrobcu, ktoré môžete nájsť na odkazoch v časti 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.

Zdroje

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-004_en.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-157-02

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

Identifikátor

OpenProject - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja OpenProject vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom analýzy obsahu robots.txt získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2023-33960

Zasiahnuté systémy

OpenProject vo verzii staršej ako 12.5.6

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

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

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2023-33960
https://github.com/opf/openproject/security/advisories/GHSA-xjfc-fqm3-95q8

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
Naša značka:
01794/2022/SK-CERT-1182

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

Identifikátor

Brocade produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Brocade vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2019-10208

Zasiahnuté systémy

Rodina produktov Brocade s komponentom PostgreSQL vo verzii staršej ako 9.4.24, 9.5.19, 9.6.15, 10.10 a 11.5

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://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/22185

BEZPEČNOSTNÝ BULLETIN

Týždeň 07. 06. 2023 - 13. 06. 2023

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

Identifikátor

Grafana - dve bezpečnostné zraniteľnosti

Popis

Vývojári aplikácie Grafana vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

06.06.2023

CVE

CVE-2023-2183, CVE-2023-2801

Zasiahnuté systémy

Grafana vo verzii staršej ako 9.4.12, 9.5.3

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://grafana.com/security/security-advisories/cve-2023-2183/
https://grafana.com/security/security-advisories/cve-2023-2801/
https://exchange.xforce.ibmcloud.com/vulnerabilities/257435
https://exchange.xforce.ibmcloud.com/vulnerabilities/257423

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
Naša značka:
01794/2022/SK-CERT-1182

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

Identifikátor

Advantech WebAccess/SCADA - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Advantech vydala bezpečnostnú aktualizáciu na svoj produkt WebAccess Node, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.06.2023

CVE

CVE-2023-22450, CVE-2023-32540, CVE-2023-32628

Zasiahnuté systémy

WebAccess/SCADA vo verzii staršej ako v9.1.4

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.

Zdroje

https://nvd.nist.gov/vuln/detail/CVE-2023-22450
https://www.cisa.gov/news-events/ics-advisories/icsa-23-152-01
https://www.cybersecurity-help.cz/vdb/SB2023060213

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

ZTE MF286R router - zero-day bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zero-day zraniteľnosti routera ZTE MF286R.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

07.06.2023

CVE

CVE-2023-32180

Zasiahnuté systémy

ZTE MF286R vo všetkých verziách firmvéru

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostnej záplaty vykonať aktualizáciu zasiahnutých systémov.
Do vydania bezpečnostných aktualizácií odporúčame limitovať prístup k administratívnemu rozhraniu routera.

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-23-818/