BEZPEČNOSTNÝ BULLETIN

Týždeň 22. 11. 2023 - 28. 11. 2023

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
Naša značka:
01794/2022/SK-CERT-1426

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

Identifikátor

Mozilla produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v prehliadači Mozilla Firefox, 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

21.11.2023

CVE

CVE-2023-49060, CVE-2023-49061, CVE-2023-6204, CVE-2023-6205, CVE-2023-6206, CVE-2023-6207, CVE-2023-6208, CVE-2023-6209, CVE-2023-6210, CVE-2023-6211, CVE-2023-6212, CVE-2023-6213

Zasiahnuté systémy

Firefox vo verzii staršej ako 120
Firefox ESR vo verzii staršej ako 115.5.0
Firefox pre vo verzii staršej ako iOS 120
Thunderbird vo verzii staršej ako 115.5

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.
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/mfsa2023-50/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-49/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-51/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-52/
https://exchange.xforce.ibmcloud.com/vulnerabilities/271993

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-1426

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

Identifikátor

NETGEAR ProSAFE Network Management System - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoj produkt ProSAFE Network Management System, ktorá opravuje dve bezpečnostné zraniteľnosti.
Zraniteľnosti nachádzajúce sa vo funkciách clearAlertByIds a getNodesByTopologyMapSearch spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvoreného reťazca vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

20.11.2023

CVE

-

Zasiahnuté systémy

ProSAFE Network Management System vo verzii staršej ako 1.7.0.31

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://kb.netgear.com/000065866/Security-Advisory-for-Multiple-Vulnerabilities-on-the-NMS300-PSV-2023-0114-PSV-2023-0115
https://www.zerodayinitiative.com/advisories/ZDI-23-1718/
https://www.zerodayinitiative.com/advisories/ZDI-23-1717/

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

Identifikátor

Zephyr - viacero bezpečnostných zraniteľností

Popis

Vývojári projektu Zephyr vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne upravených paketov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.11.2023

CVE

CVE-2023-3725, CVE-2023-4257, CVE-2023-4258, CVE-2023-4259, CVE-2023-4260, CVE-2023-4263, CVE-2023-4264, CVE-2023-4424, CVE-2023-5055, CVE-2023-5139, CVE-2023-5184, CVE-2023-5563

Zasiahnuté systémy

Zephyr vo verzii staršej ako 3.5.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
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://docs.zephyrproject.org/3.5.0/releases/release-notes-3.5.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/272100

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

Identifikátor

Fuji Electric Tellus Lite V-Simulator - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Fuji Electric vydala bezpečnostnú aktualizáciu na svoj produkt Tellus Lite V-Simulator, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov 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

21.11.2023

CVE

CVE-2023-35127, CVE-2023-40152, CVE-2023-5299

Zasiahnuté systémy

Tellus Lite V-Simulator vo verzii staršej ako 4.0.19.0.

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://www.cisa.gov/news-events/ics-advisories/icsa-23-325-02
https://exchange.xforce.ibmcloud.com/vulnerabilities/272023
https://exchange.xforce.ibmcloud.com/vulnerabilities/272026
https://exchange.xforce.ibmcloud.com/vulnerabilities/272027

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

Identifikátor

Apache DolphinScheduler - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Apache DolphinScheduler 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 získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.11.2023

CVE

CVE-2023-48796, CVE-2023-49068

Zasiahnuté systémy

Apache DolphinScheduler vo verzii staršej ako 3.0.2

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://www.openwall.com/lists/oss-security/2023/11/24/2
https://www.openwall.com/lists/oss-security/2023/11/24/1
https://exchange.xforce.ibmcloud.com/vulnerabilities/272208
https://exchange.xforce.ibmcloud.com/vulnerabilities/272251

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

Identifikátor

Headwind MDM Web panel - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Headwind MDM Web panel. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať prístup k hodnote JWT SECRET a následne spôsobiť narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.11.2023

CVE

CVE-2023-47312, CVE-2023-47314, CVE-2023-47315, CVE-2023-47316

Zasiahnuté systémy

Headwind MDM Web panel vo verzii staršej ako 5.22.1 (vrátane)

Následky

Narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

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://boltonshield.com/en/cve/cve-2023-47315/
https://exchange.xforce.ibmcloud.com/vulnerabilities/272177
https://exchange.xforce.ibmcloud.com/vulnerabilities/272178
https://exchange.xforce.ibmcloud.com/vulnerabilities/272176
https://exchange.xforce.ibmcloud.com/vulnerabilities/272168

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

Identifikátor

Dell Command a OS Recovery Tool - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Dell vydala bezpečnostné aktualizácie na produkty Command a OS Recovery Tool, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v aplikácii Dell Command, 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 zneprístupnenie služby.

Dátum prvého zverejnenia varovania

22.11.2023

CVE

CVE-2023-39253, CVE-2023-43086, CVE-2023-44289, CVE-2023-44290

Zasiahnuté systémy

Dell Command Configure vo verzii staršej ako 4.11.0.70, A00
Dell Command Monitor vo verzii staršej ako 10.10.0.39, A00
Dell OS Recovery Tool vo verzii staršej ako 2.3.7523.0

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://www.dell.com/support/kbdoc/en-us/000218424/dsa-2023-387-security-update-for-a-dell-command-configure-vulnerability
https://www.dell.com/support/kbdoc/en-us/000218628/dsa-2023-390-security-update-for-dell-command-configure-and-dell-command-monitor-vulnerabilities
https://www.dell.com/support/kbdoc/en-us/000217699/dsa-2023-336-security-update-for-a-dell-os-recovery-tool-vulnerability

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

Identifikátor

Zoho ManageEngine Recovery Manager Plus

Popis

Divízia ManageEngine spoločnosti Zoho vydala bezpečnostnú aktualizáciu na svoj produkt Recovery Manager Plus, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť sa nachádza v implementácii metódy getEscapedValue, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvoreného reťazca vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.11.2023

CVE

CVE-2023-48646

Zasiahnuté systémy

RecoveryManager Plus vo verzii staršej ako 6070

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.manageengine.com/ad-recovery-manager/advisory/CVE-2023-48646.html
https://www.zerodayinitiative.com/advisories/ZDI-23-1719/

Dôležitosť	☒ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 2.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WAGO zariadenia - bezpečnostná zraniteľnosť

Popis

Spoločnosť WAGO vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

21.11.2023

CVE

CVE-2023-4089

Zasiahnuté systémy

Compact Controller CC100, Edge Controller, PFC100, PFC200, Touch Panel 600 standard, marine a advanced line vo verzii firmvéru staršej ako FW26

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://cert.vde.com/de/advisories/VDE-2023-046/
https://www.cisa.gov/news-events/ics-advisories/icsa-23-325-01
https://exchange.xforce.ibmcloud.com/vulnerabilities/269454