BEZPEČNOSTNÝ BULLETIN

Týždeň 04. 10. 2023 - 10. 10. 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-1362

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

Identifikátor

Google Chrome - bezpečnostná zraniteľnosť

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Google Chrome, ktorá opravuje bezpečnostnú zraniteľnosť.
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

09.10.2023

CVE

CVE-2023-5346

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 117.0.5938.149
Chrome pre Windows vo verzii staršej ako 117.0.5938.149/.150

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/2023/10/stable-channel-update-for-desktop.html
https://nvd.nist.gov/vuln/detail/CVE-2023-5346

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

Identifikátor

Cacti - dve bezpečnostné zraniteľnosti

Popis

Vývojári nástroja Cacti vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.10.2023

CVE

CVE-2023-39365

Zasiahnuté systémy

Cacti vo verzii staršej ako 1.2.25

Následky

Eskalácia privilégií
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.zerodayinitiative.com/advisories/ZDI-23-1500/
https://www.zerodayinitiative.com/advisories/ZDI-23-1499/
https://github.com/cacti/cacti/security/advisories/GHSA-v5w7-hww7-2f22

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

Identifikátor

Apache NiFi - tri bezpečnostné zraniteľnosti

Popis

Vývojári projektu Apache NiFi vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov 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

29.09.2023

CVE

CVE-2023-34468, CVE-2023-36542, CVE-2023-40037

Zasiahnuté systémy

Apache NiFi vo verzii staršej ako 1.23.1

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://nifi.apache.org/security.html#1.23.1
https://www.securityweek.com/hackers-set-sights-on-apache-nifi-flaw-that-exposes-many-organizations-to-attacks/

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

Identifikátor

A10 Thunder ADC - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť A10 Networks vydala bezpečnostnú aktualizáciu na svoj produkt A10 Thunder ADC, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom symbolického odkazu získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

12.09.2023

CVE

CVE-2023-42129, CVE-2023-42130

Zasiahnuté systémy

A10 Thunder ADC vo verzii staršej ako 6.0.2 HF-20230006.upg
A10 Thunder ADC vo verzii staršej ako 5.2.1-P9 HF-20230006.upg
A10 Thunder ADC vo verzii staršej ako 5.2.1-P9 (vrátane, je potrebné aktualizovať ACOS)
A10 Thunder ADC vo verzii staršej ako 4.1.4-GR1-P13 HF-20230006.upg
A10 Thunder ADC vo verzii staršej ako 4.1.4-GR1-P13 (vrátane, je potrebné aktualizovať ACOS)

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://support.a10networks.com/support/security_advisory/a10-acos-file-access-vulnerability/
https://www.zerodayinitiative.com/advisories/ZDI-23-1496/
https://www.zerodayinitiative.com/advisories/ZDI-23-1495/

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

Identifikátor

BMC IPMI firmware - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Supermicro vydala bezpečnostnú aktualizáciu na svoj firmvér pre základné dosky, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, neautentifikovanému útočníkovi prostredníctvom XSS (Cross Site Scripting) útoku vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľností vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

06.10.2023

CVE

CVE-2023-40284, CVE-2023-40285, CVE-2023-40286, CVE-2023-40287, CVE-2023-40288, CVE-2023-40289, CVE-2023-40290

Zasiahnuté systémy

Supermicro BMC vo vybraných základných doskách X11, H11, B11, CMM, M11 a H12

Následky

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

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://www.supermicro.com/en/support/security_BMC_IPMI_Oct_2023
https://thehackernews.com/2023/10/supermicros-bmc-firmware-found.html

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

Identifikátor

G Data Total Security - bezpečnostná zraniteľnosť

Popis

Spoločnosť G Data vydala bezpečnostnú aktualizáciu na svoj produkt Total Security, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom podvrhnutia špeciálne vytvoreného symbolického odkazu eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.09.2023

CVE

CVE-2023-42126

Zasiahnuté systémy

G Data Total Security vo verzii staršej ako 25.5.16.125

Následky

Eskalácia privilégií
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/267466
https://www.zerodayinitiative.com/advisories/ZDI-23-1493/

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

Identifikátor

GNU C Library - bezpečnostná zraniteľnosť

Popis

Vývojári knižnice GNU C 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 pretečenia zásobníka 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

03.10.2023

CVE

CVE-2023-4911

Zasiahnuté systémy

glibc vo verzii staršej ako 2.35

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.qualys.com/2023/10/03/cve-2023-4911/looney-tunables-local-privilege-escalation-glibc-ld-so.txt
https://access.redhat.com/security/cve/cve-2023-4911
https://nvd.nist.gov/vuln/detail/CVE-2023-4911
https://github.com/RickdeJager/CVE-2023-4911

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

Identifikátor

Mali GPU Driver - tri bezpečnostné zraniteľnosti

Popis

Vývojári ovládača Mali GPU vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.
Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

02.10.2023

CVE

CVE-2023-33200, CVE-2023-34970, CVE-2023-4211

Zasiahnuté systémy

Bifrost, Valhall a Arm 5th Gen GPU Architectur Kernel Driver vo verzii staršej ako r43p0

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://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities
https://www.tenable.com/cve/CVE-2023-4211
https://thehackernews.com/2023/10/arm-issues-patch-for-mali-gpu-kernel.html

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

Identifikátor

OpenRefine - bezpečnostná zraniteľnosť

Popis

Vývojári nástroja OpenRefine vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených TAR súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.10.2023

CVE

CVE-2023-37476

Zasiahnuté systémy

OpenRefine vo verzii staršej ako 3.7.4

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://github.com/OpenRefine/OpenRefine/releases/tag/3.7.4
https://thehackernews.com/2023/10/openrefines-zip-slip-vulnerability.html

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

Identifikátor

WebM Project Libvpx - bezpečnostná zraniteľnosť

Popis

Vývojári projektu Libvpx vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
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

30.09.2023

CVE

CVE-2023-44488

Zasiahnuté systémy

libvpx vo verzii staršej ako 1.13.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/267474
https://github.com/webmproject/libvpx/releases/tag/v1.13.1

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

NPort 5000 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktov série NPort 5000.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.10.2023

CVE

CVE-2023-4929

Zasiahnuté systémy

NPort 5000AI-M12 Series vo verzii staršej ako 1.5 (vrátane)
NPort 5100 Series (NPort 5130/5150 modely) vo verzii staršej ako 3.10 (vrátane)
NPort 5100 Series (NPort 5110 modely) vo verzii staršej ako 2.10 (vrátane)
NPort 5100A Series vo verzii staršej ako 1.6 (vrátane)
NPort 5200 Series vo verzii staršej ako 2.12 (vrátane)
NPort 5200A Series vo verzii staršej ako 1.6 (vrátane)
NPort 5410/5430 (Rev. 3.2 a neskoršie) a NPort 5450 (all Rev.) vo verzii staršej ako 3.14 (vrátane)
NPort 5410/5430 (Rev 2.x a skoršie) vo verzii staršej ako 2.9 (vrátane)
NPort 5600 Series vo verzii staršej ako 3.11 (vrátane)
NPort 5600-DT Series vo verzii staršej ako 2.9 (vrátane)
NPort IA5000 Series (hardware version 2.0 a neskoršie) vo verzii staršej ako 2.1 (vrátane)
NPort IA5000 Series (hardware version 1.x) vo verzii staršej ako 1.7 (vrátane)
NPort IA5000A Series (NPort IA5450A Series) vo verzii staršej ako 2.0 (vrátane)
NPort IA5000A Series (NPort IA5150A/IA5250A Series) vo verzii staršej ako 1.5 (vrátane)
NPort IA5000A-I/O Series vo verzii staršej ako 2.0 (vrátane)
NPort IAW5000A-I/O Series vo verzii staršej ako 2.2 (vrátane)
NPort P5150A Series vo verzii staršej ako 1.6 (vrátane)

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

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-1362

Odporúčania
Výrobca uviedol, že na predmetnú zraniteľnosť nie je možné vydať bezpečnostnú záplatu a odporúča postupovať podľa pokynov, ktoré môžete nájsť na webovej stránke spoločnosti MOXA: https://www.moxa.com/getmedia/67b5e549-a125-4a6a-b99b-23017c75cfc1/moxa-the-security-hardening-guide-for-the-nport-5000-series-tech-note-v1.1.pdf 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.moxa.com/en/support/product-support/security-advisory/mpsa-233328-nport-5000-series-firmware-improper-validation-of-integrity-check-vulnerability