BEZPEČNOSTNÝ BULLETIN

Týždeň 20. 09. 2023 - 26. 09. 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-1343

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

Identifikátor

Atos Unify OpenScape - bezpečnostná zraniteľnosť

Popis

Spoločnosť Atos 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 zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

18.09.2023

CVE

CVE-2023-36618

Zasiahnuté systémy

OpenScape SBC vo verzii staršej ako R3.3.0
OpenScape Branch vo verzii staršej ako R3.3.0
OpenScape BCF vo verzii staršej ako R10.10.0

Následky

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

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/266337

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

Identifikátor

Nagios XI - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Nagios vydala bezpečnostnú aktualizáciu na svoj produkt Nagios XI, ktorá opravuje 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

11.09.2023

CVE

CVE-2023-40931, CVE-2023-40932, CVE-2023-40933, CVE-2023-40934

Zasiahnuté systémy

Nagios XI vo verzii staršej ako 5.11.2

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.nagios.com/downloads/nagios-xi/change-log/
https://outpost24.com/blog/nagios-xi-vulnerabilities/

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

Identifikátor

Qnap produkty - bezpečnostná zraniteľnosť

Popis

Spoločnosť Qnap vydala bezpečnostné aktualizácie na svoje produkty QTS, QuTS hero, QuTScloud a Multimedia Console, ktoré opravujú bezpečnostnú zraniteľnosť.
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

16.09.2023

CVE

CVE-2023-23362, CVE-2023-23363

Zasiahnuté systémy

QTS vo verzii staršej ako 4.3.6.2441 build 20230621
QTS vo verzii staršej ako 4.3.4.2451 build 20230621
QTS vo verzii staršej ako 4.3.3.2420 build 20230621
QTS vo verzii staršej ako 4.2.6 build 20230621
QTS vo verzii staršej ako 4.5.4.2374 build 20230416
QTS vo verzii staršej ako 5.0.1.2376 build 20230421
QuTS hero vo verzii staršej ako h4.5.4.2374 build 20230417
QuTS hero vo verzii staršej ako h5.0.1.2376 build 20230421
QuTScloud vo verzii staršej ako c5.0.1.2374
Multimedia Console vo verzii staršej ako 2.1.1 (2023/03/29)
Multimedia Console vo verzii staršej ako 1.4.7 (2023/03/20)

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.qnap.com/en/security-advisory/qsa-23-18
https://www.cyberveille-sante.gouv.fr/alertes/qnap-cve-2023-23362-2023-09-18
https://www.qnap.com/en/security-advisory/qsa-23-25
https://www.qnap.com/en/security-advisory/qsa-23-29

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

Identifikátor

Moveit Transfer - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Moveit vydala bezpečnostnú aktualizáciu na svoj produkt Moveit Transfer, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom SQL injekcie získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.09.2023

CVE

CVE-2023-40043, CVE-2023-42656, CVE-2023-42660

Zasiahnuté systémy

MOVEit Transfer 2023 vo verzii staršej ako 2023.0.6 (15.0.6)
MOVEit Transfer 2022 vo verzii staršej ako 2022.1.9 (14.1.9)
MOVEit Transfer 2022 vo verzii staršej ako 2022.0.8 (14.0.8)
MOVEit Transfer 2021 vo verzii staršej ako 2021.1.8 (13.1.8)
MOVEit Transfer 2021 vo verzii staršej ako 2021.0.x (13.0.x)

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://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-September-2023

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Atlassian Bitbucket & Confluence - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Atlassian 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.09.2023

CVE

CVE-2022-25647, CVE-2023-22512, CVE-2023-22513, CVE-2023-28709

Zasiahnuté systémy

Jira Service Management Server and Data Center vo verzii staršej ako 4.20.25, 5.4.9, 5.9.2, 5.10.1, 5.11.0
Confluence Server and Data Center vo verzii staršej ako 7.19.13, 7.19.14, 8.5.1, 8.6.0
Bitbucket Server and Data Center vo verzii staršej ako 8.9.5, 8.10.5, 8.11.4, 8.12.2, 8.13.1, 8.14.0
Bamboo Server and Data Center vo verzii staršej ako 9.2.4, 9.3.1

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 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://confluence.atlassian.com/security/security-bulletin-september-19-2023-1283691616.html
https://jira.atlassian.com/browse/BSERV-14419

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

XenSource Xen - bezpečnostná zraniteľnosť

Popis

Vývojári hypervízora Xen vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.09.2023

CVE

CVE-2023-34322

Zasiahnuté systémy

Xen vo verzii staršej ako xsa438-4.17.patch
Xen vo verzii staršej ako xsa438-4.16.patch
Xen vo verzii staršej ako xsa438-4.15.patch

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

http://xenbits.xen.org/xsa/advisory-438.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/266513

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

Identifikátor

Drupal Core - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Drupal Core 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 získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.09.2023

CVE

-

Zasiahnuté systémy

Drupal Core vo verzii staršej ako 9.5.11, 10.0.11 a 10.1.4

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na redakčnom systéme Drupal v zraniteľnej verzii. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu redakčného systému a všetkých používaných pluginov.
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.drupal.org/sa-core-2023-006
https://exchange.xforce.ibmcloud.com/vulnerabilities/266610

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

Identifikátor

Autodesk produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Autodesk vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte AutoCad, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky alebo súboru vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

24.08.2023

CVE

CVE-2023-29073, CVE-2023-29074, CVE-2023-29075, CVE-2023-29076, CVE-2023-41139, CVE-2023-41140

Zasiahnuté systémy

Autodesk AutoCAD vo verzii staršej ako 2023.1.4
Autodesk® AutoCAD® Architecture vo verzii staršej ako 2023.1.4
Autodesk® AutoCAD® Electrical vo verzii staršej ako 2023.1.4
Autodesk® AutoCAD® Map 3D vo verzii staršej ako 2023.1.4
Autodesk® AutoCAD® Mechanical vo verzii staršej ako 2023.1.4
Autodesk® AutoCAD® MEP vo verzii staršej ako 2023.1.4
Autodesk® AutoCAD® Plant 3D vo verzii staršej ako 2023.1.4
Autodesk® AutoCAD LT® vo verzii staršej ako 2023.1.4
Autodesk AutoCAD Mac vo verzii staršej ako 2024.1
Autodesk AutoCAD LT for Mac vo verzii staršej ako 2024.1
Autodesk Civil 3D vo verzii staršej ako 2023.1.4
Autodesk Advance Steel vo verzii staršej ako 2023.1.4

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.
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-23-1442/ https://www.autodesk.com/trust/security-advisories/adsk-sa-2023-0018

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

Identifikátor

Foxconn Live Update Utility - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Foxconn Live Update Utility. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.09.2023

CVE

CVE-2020-24088

Zasiahnuté systémy

Foxconn Live Update Utility vo verzii staršej ako 2.1.6.26 (vrátane)

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/266533
https://github.com/rjt-gupta/CVE-2020-24088

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

Identifikátor

Intel Driver & Support Assistant - zero-day bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zero-day zraniteľnosti produktu Intel Driver & Support Assistant.
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

25.09.2023

CVE

CVE-2023-42099

Zasiahnuté systémy

Intel Driver & Support Assistant vo verzii staršej ako 23.3.25 (vrátane)

Následky

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

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť 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-23-1449/

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

Identifikátor

Delta Electronics DIAScreen - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Electronics vydala bezpečnostnú aktualizáciu na svoj produkt DIAScreen, ktorá opravuje bezpečnostnú zraniteľnosť.
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

21.09.2023

CVE

CVE-2023-5068

Zasiahnuté systémy

DIAScreen vo verzii staršej ako v1.3.2

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.cisa.gov/news-events/ics-advisories/icsa-23-264-03

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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

22.09.2023

CVE

CVE-2023-42753

Zasiahnuté systémy

Linux Kernel vo verzii upstream, 6.1, 5.15, a 5.10 bez commitu 886503f34d63

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://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=050d91c03b28ca479df13dfb02bcd2c60dd6a878
https://seclists.org/oss-sec/2023/q3/216
https://exchange.xforce.ibmcloud.com/vulnerabilities/266809

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

Identifikátor

ISC BIND - bezpečnostná zraniteľnosť

Popis

Spoločnosť ISC vydala bezpečnostné aktualizácie na svoj open-source softvér BIND, ktoré opravujú dve bezpečnostné zraniteľnosti.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej správy spôsobiť znneprístupnenie služby.

Dátum prvého zverejnenia varovania

20.09.2023

CVE

CVE-2023-3341, CVE-2023-4236

Zasiahnuté systémy

BIND 9 vo verzii staršej ako 9.16.44, 9.18.19 a 9.19.17

BIND Supported Preview Edition vo verzii staršej ako 9.16.44-S1 a 9.18.19-S1

Následky

Znneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://kb.isc.org/v1/docs/cve-2023-4236
https://kb.isc.org/v1/docs/cve-2023-3341
https://exchange.xforce.ibmcloud.com/vulnerabilities/266515

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

Identifikátor

D-Link DIR-806 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu D-Link DIR-806.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.09.2023

CVE

CVE-2023-43128

Zasiahnuté systémy

D-Link DIR-806 vo verzii firmvéru staršej ako DIR806A1_FW100CNb11 (vrátane)

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 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/266787

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

Identifikátor

SolarWinds Platform - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť SolarWinds vydala bezpečnostnú aktualizáciu na svoj produkt SolarWinds Platform, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.09.2023

CVE

CVE-2023-23840, CVE-2023-23845

Zasiahnuté systémy

SolarWinds Platform vo verzii staršej ako 2023.3.1

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://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2023-3-1_release_notes.htm
https://nvd.nist.gov/vuln/detail/CVE-2023-23840

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-1343