BEZPEČNOSTNÝ BULLETIN

Týždeň 03. 05. 2023 - 09. 05. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Foxit PDF Reader a Editor - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	NETGEAR RAX30 - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Junos OS a Junos OS Evolved - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Apache Spark - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
05.	Google Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
06.	Zyxel routre - bezpečnostná zraniteľnosť	Vysoká	**8.8**
07.	D-Link produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
08.	Canon tlačiarne - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
09.	Illumos-gate - bezpečnostná zraniteľnosť	Vysoká	**8.8**
10.	PHPJabbers Simple CMS - bezpečnostná zraniteľnosť	Vysoká	**8.8**
11.	WordPress Advanced Custom Fields Pro Plugin - bezpečnostná zraniteľnosť	Vysoká	**8.8**
12.	Apache Airflow - bezpečnostná zraniteľnosť	Vysoká	**8.8**
13.	Newsletter plugin pre WordPress - bezpečnostná zraniteľnosť	Vysoká	**8.8**
14.	NETGEAR ProSAFE® NMS300 - dve bezpečnostné zraniteľnosti	Vysoká	**8.8**
15.	Mozilla produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
16.	Qualcomm chipsety - viacero bezpečnostných zraniteľností	Vysoká	**8.4**
17.	Apache bRPC - bezpečnostná zraniteľnosť	Vysoká	**8.3**
18.	F5 NGINX - viacero bezpečnostných zraniteľností	Vysoká	**8.1**
19.	Apple Slúchadlá - bezpečnostná zraniteľnosť	Vysoká	**8.1**
20.	Google Android - viacero bezpečnostných zraniteľností	Vysoká	**7.9**
21.	Linux Kernel - bezpečnostná zraniteľnosť	Vysoká	**7.8**
22.	Cisco IOS XE Software IOx Application - bezpečnostná zraniteľnosť	Vysoká	**7.8**
23.	FRRouting (Border Gateway Protocol) - tri bezpečnostné zraniteľnosti	Stredná	**6.5**
24.	Tenda N301 - dve bezpečnostné zraniteľnosti	Stredná	**6.5**

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-1129

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

Identifikátor

Foxit PDF Reader a Editor - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit Software vydala bezpečnostné aktualizácie na produkty PDF Reader a Editor, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

19.04.2023

CVE

CVE-2023-27363, CVE-2023-27364, CVE-2023-27365, CVE-2023-27366

Zasiahnuté systémy

Foxit PDF Reader vo verzii staršej ako 12.1.2
Foxit PDF Editor vo verzii staršej ako 12.1.2

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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-23-494/
https://www.zerodayinitiative.com/advisories/ZDI-23-493/
https://www.zerodayinitiative.com/advisories/ZDI-23-492/
https://www.zerodayinitiative.com/advisories/ZDI-23-491/

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

Identifikátor

NETGEAR RAX30 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NETGEAR vydala bezpečnostnú aktualizáciu na svoj router RAX30, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.05.2023

CVE

CVE-2023-27356, CVE-2023-27357, CVE-2023-27358, CVE-2023-27360, CVE-2023-27361, CVE-2023-27367, CVE-2023-27368, CVE-2023-27369, CVE-2023-27370

Zasiahnuté systémy

NETGEAR RAX30 s firmvérom vo verzii staršej ako 1.0.10.94

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do 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-23-503/
https://www.zerodayinitiative.com/advisories/ZDI-23-502/
https://www.zerodayinitiative.com/advisories/ZDI-23-501/
https://www.zerodayinitiative.com/advisories/ZDI-23-500/
https://www.zerodayinitiative.com/advisories/ZDI-23-499/
https://www.zerodayinitiative.com/advisories/ZDI-23-498/
https://www.zerodayinitiative.com/advisories/ZDI-23-497/
https://www.zerodayinitiative.com/advisories/ZDI-23-496/
https://www.zerodayinitiative.com/advisories/ZDI-23-495/

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

Identifikátor

Junos OS a Junos OS Evolved - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Juniper vydala bezpečnostné aktualizácie na operačné systémy Junos OS a Junos OS Evolved, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.05.2023

CVE

CVE-2013-5211, CVE-2015-5146, CVE-2015-7973, CVE-2015-7974, CVE-2015-7975, CVE-2015-7976, CVE-2015-7977, CVE-2015-7978, CVE-2015-7979, CVE-2015-8138, CVE-2015-8139, CVE-2015-8140, CVE-2015-8158, CVE-2016-1547, CVE-2016-1548, CVE-2016-1550, CVE-2016-1551, CVE-2016-2516, CVE-2016-2517, CVE-2016-2518, CVE-2016-2519, CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, CVE-2016-4957, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9042, CVE-2016-9310, CVE-2016-9311, CVE-2016-9312, CVE-2017-6451, CVE-2017-6452, CVE-2017-6455, CVE-2017-6458, CVE-2017-6459, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2023-22396

Zasiahnuté systémy

Junos OS vo verziách starších ako 12.3R12-S15, 12.3X48-D95, 14.1X53-D53, 15.1R7-S6, 15.1X49-D190, 16.1R7-S6, 16.2R3, 17.1R2-S11, 17.1R3-S1, 17.2R1-S9, 17.2R2-S8, 17.2R3-S3, 17.3R2-S5, 17.3R3-S6, 17.4R2-S7, 17.4R3, 18.1R3-S8, 18.2R2-S7, 18.2R3-S1, 18.3R1-S5, 18.3R2-S2, 18.3R3, 18.4R1-S4, 18.4R2-S1, 18.4R3, 19.1R1-S3, 19.1R2, 19.2R1-S1, 19.2R2, a 19.3R1
Junos OS Evolved vo verzii staršej ako 20.1R1-EVO

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://supportportal.juniper.net/s/article/2021-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-NTP-vulnerabilities-resolved?language=en_US https://supportportal.juniper.net/s/article/2017-04-Security-Bulletin-Junos-Multiple-vulnerabilities-in-NTP-VU-633847?language=en_US

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

Identifikátor

Apache Spark - dve bezpečnostné zraniteľnosti

Popis

Vývojári nástroja Apache Spark 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 zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.05.2023

CVE

CVE-2022-33891, CVE-2023-32007

Zasiahnuté systémy

Apache Spark vo verzii staršej ako 3.4.0

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/254113
https://lists.apache.org/thread/poxgnxhhnzz735kr1wos366l5vdbb0nv

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 bezpečnostné aktualizácie na svoj prehliadač Chrome, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

02.05.2023

CVE

CVE-2023-2459, CVE-2023-2460, CVE-2023-2461, CVE-2023-2462, CVE-2023-2463, CVE-2023-2464, CVE-2023-2465, CVE-2023-2466, CVE-2023-2467, CVE-2023-2468

Zasiahnuté systémy

Chrome pre Android vo verzii staršej ako 113.0.5672.76/.77
Chrome pre Windows vo verzii staršej ako 113.0.5672.63/.64
Chrome pre Mac & Linux vo verzii staršej ako 113.0.5672.63

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://chromereleases.googleblog.com/
https://exchange.xforce.ibmcloud.com/vulnerabilities/254157

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

Identifikátor

Zyxel routre - bezpečnostná zraniteľnosť

Popis

Spoločnosť Zyxel vydala bezpečnostné aktualizácie na routre NBG6604 a NBG-418N, 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 HTTP požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

02.05.2023

CVE

CVE-2023-22919, CVE-2023-22921, CVE-2023-22922, CVE-2023-22923, CVE-2023-22924

Zasiahnuté systémy

NBG6604 vo verzii staršej ako V1.01(ABIR.1)C0
NBG-418N v2 vo verzii staršej ako V1.00(AARP.14)C0

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/254232
https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-vulnerability-in-nbg6604-home-router
https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-nbg-418n-v2-home-router

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

Identifikátor

D-Link produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť D-Link vydala bezpečnostné aktualizácie firmvéru pre routre DAP-1360, DIR-2640 a DAP-2020, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.05.2023

CVE

CVE-2023-32136, CVE-2023-32138, CVE-2023-32139, CVE-2023-32140, CVE-2023-32141, CVE-2023-32142, CVE-2023-32143, CVE-2023-32144, CVE-2023-32145, CVE-2023-32146, CVE-2023-32147, CVE-2023-32148, CVE-2023-32149, CVE-2023-32150, CVE-2023-32151, CVE-2023-32152

Zasiahnuté systémy

D-Link DAP-1360 vo verzii firmvéru staršej ako v6.15EUb01_Beta_Hotfix
D-Link DIR-2640 vo verzii firmvéru staršej ako v1.11B02_Beta_Hotfix
D-Link DAP-2020 vo verzii firmvéru staršej ako v1.03rc004_Beta_Hotfix

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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10324
https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10323
https://www.zerodayinitiative.com/advisories/ZDI-23-528/

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

Identifikátor

Canon tlačiarne - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Canon vydala bezpečnostné aktualizácie firmvéru na svoje portfólio tlačiarní, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom pretečenia zásobníka vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

26.04.2023

CVE

CVE-2022-43608, CVE-2022-43974, CVE-2023-0851, CVE-2023-0852, CVE-2023-0853, CVE-2023-0854, CVE-2023-0855, CVE-2023-0856, CVE-2023-0857, CVE-2023-0858, CVE-2023-0859

Zasiahnuté systémy

MF1127C
MF641CW/MF642CDW/MF644CDW
MF741CDW/MF743CDW/MF745CDW/MF746CDW
LBP1127C
LBP622CDW/LBP623CDW
LBP664CDW
TC-20*/TC-20M
G3270*
GX3020*/GX4020*

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.usa.canon.com/support/canon-product-advisories/Service-Notice-Vulnerabilities-Remediation-Against-Buffer-Overflow
https://www.zerodayinitiative.com/advisories/ZDI-23-549/

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

Identifikátor

Illumos-gate - bezpečnostná zraniteľnosť

Popis

Vývojári open-source Unixového operačného systému illumos-gate 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 zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

04.05.2023

CVE

CVE-2023-31284

Zasiahnuté systémy

illumos-gate vo všetkých verziách

Následky

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

Odporúčania

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

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/254456

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

Identifikátor

PHPJabbers Simple CMS - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti Simple CMS.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód a získať neoprávený prístup k citlivým údajom.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

03.05.2023

CVE

-

Zasiahnuté systémy

PHPJabbers Simple CMS vo verzii staršej ako 5.0 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné 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 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/254423
https://packetstormsecurity.com/files/172115

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

Identifikátor

WordPress Advanced Custom Fields Pro Plugin - bezpečnostná zraniteľnosť

Popis

Vývojári Wordpress pluginu Advanced Custom Fields Pro vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku vykonať škodlivý kód a získať neoprávnený prístup k citlivým údajom.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

05.05.2023

CVE

CVE-2023-30777

Zasiahnuté systémy

WordPress Advanced Custom Fields Pro Plugin vo verzii staršej ako 6.1.6.

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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://securityonline.info/cve-2023-30777-xss-flaw-found-in-wordpress-plugin-with-more-than-2-million-installations/
https://thehackernews.com/2023/05/new-vulnerability-in-popular-wordpress.html

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

Identifikátor

Apache Airflow - bezpečnostná zraniteľnosť

Popis

Vývojári platformy pre workflow manažment Apache Airflow 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 zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

08.05.2023

CVE

CVE-2023-25754

Zasiahnuté systémy

Apache Airflow vo verzii staršej ako 2.6.0

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://exchange.xforce.ibmcloud.com/vulnerabilities/254655

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

Identifikátor

Newsletter plugin pre WordPress - bezpečnostná zraniteľnosť

Popis

Vývojári Wordpress pluginu Newsletter vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom cross-site scripting (XSS) útoku získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

10.05.2023

CVE

CVE-2023-27922

Zasiahnuté systémy

Newsletter vo verzii staršej ako 7.6.9

Následky

Vykonanie škodlivého kódu
Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky založené na redakčnom systéme Wordpress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, administrátorom odporúčamy vykonať aktualizáciu zasiahnutých systémov.

Zdroje

http://jvn.jp/en/jp/JVN59341308/index.html
https://wordpress.org/plugins/newsletter/#developers

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

Identifikátor

NETGEAR ProSAFE® NMS300 - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu ProSAFE® Network Management System.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, 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

02.05.2023

CVE

-

Zasiahnuté systémy

ProSAFE® Network Management System (NMS300) vo verzii staršej ako 1.7.0.12 (vrátane)

Následky

Eskalácia privilégií
Úplné 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.
V prípade, že bude pre dané zariadenie ohlásené ukončenie podpory, odporúčame prejsť na iný produkt s platnou podporou.

Zdroje

https://flashpoint.io/resources/research/fp-2023-01-netgear-prosafe-network-management-system/

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 produkty Firefox a Firefox ESR, ktoré opravujú 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

09.05.2023

CVE

CVE-2023-32205, CVE-2023-32206, CVE-2023-32207, CVE-2023-32208, CVE-2023-32209, CVE-2023-32210, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32214, CVE-2023-32215, CVE-2023-32216

Zasiahnuté systémy

Firefox ESR vo verzii staršej ako 102.11
Firefox vo verzii staršej ako 113

Následky

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

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
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.mozilla.org/en-US/security/advisories/mfsa2023-16/
https://www.mozilla.org/en-US/security/advisories/mfsa2023-17/

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 zverejnila informácie o zraniteľnostiach svojich chipsetov.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

01.05.2023

CVE

CVE-2022-25713, CVE-2022-33273, CVE-2022-33281, CVE-2022-33292, CVE-2022-33304, CVE-2022-33305, CVE-2022-34144, CVE-2022-40504, CVE-2022-40505, CVE-2022-40508, CVE-2023-21642, CVE-2023-21665, CVE-2023-21666

Zasiahnuté systémy

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v sekcii ZDROJE

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnená zmena v systéme
Neoprávnený prístup k citlivým údajom
Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, že Vaše zariadenie nevyužíva žiaden zo zasiahnutých chipsetov. V prípade, že áno, odporúčame sledovať stránku výrobcu pre Vaše konkrétne zariadenie a po vydaní príslušných záplat systémy aktualizovať.
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/may-2023-bulletin.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/254199

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

Identifikátor

Apache bRPC - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku Apache bRPC 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 zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.05.2023

CVE

CVE-2023-31039

Zasiahnuté systémy

Apache bRPC vo verzii staršej ako 1.5.0

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/254660

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

Identifikátor

F5 NGINX - viacero bezpečnostných zraniteľností

Popis

Spoločnosť F5 vydala bezpečnostné aktualizácie na produkty API Connectivity Manager, Instance Manager a Security Monitoring, 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 získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

03.05.2023

CVE

CVE-2023-28656

Zasiahnuté systémy

NGINX Instance Manager vo verzii staršej ako 2.9.0
NGINX API Connectivity Manager vo verzii staršej ako 1.5.0
NGINX Security Monitoring vo verzii staršej ako 1.3.0

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

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://my.f5.com/manage/s/article/K000133417
https://exchange.xforce.ibmcloud.com/vulnerabilities/254324

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

Identifikátor

Apple Slúchadlá - bezpečnostná zraniteľnosť

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie firmvéru pre produkty Powerbeats Pro, Beats Fit Pro, AirPods, AirPods Pro, a AirPods Max, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v dosahu Bluetooth prostredníctvom zaslania špeciálne vytvorenej požiadavky získať prístup k slúchadlám.

Dátum prvého zverejnenia varovania

02.05.2023

CVE

CVE-2023-27964

Zasiahnuté systémy

Powerbeats Pro, Beats Fit Pro s firmvérom vo verzii staršej ako 5B66
AirPods, AirPods Pro, a AirPods Max s firmvérom vo verzii staršej ako 5E133

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.apple.com/en-us/HT213752

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.9
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Google Android - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj operačný systém Android, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

03.05.2023

CVE

CVE-2021-0877, CVE-2021-39617, CVE-2022-20338, CVE-2022-20444, CVE-2022-25713, CVE-2022-33273, CVE-2022-33305, CVE-2022-34144, CVE-2022-40504, CVE-2022-40508, CVE-2022-46394, CVE-2022-46395, CVE-2022-46396, CVE-2022-46891, CVE-2022-47469, CVE-2022-47470, CVE-2022-47486, CVE-2022-47487, CVE-2022-47488, CVE-2023-0266, CVE-2023-20694, CVE-2023-20695, CVE-2023-20696, CVE-2023-20697, CVE-2023-20698, CVE-2023-20699, CVE-2023-20726, CVE-2023-20914, CVE-2023-20930, CVE-2023-20993, CVE-2023-21102, CVE-2023-21103, CVE-2023-21104, CVE-2023-21106, CVE-2023-21107, CVE-2023-21109, CVE-2023-21110, CVE-2023-21111, CVE-2023-21112, CVE-2023-21116, CVE-2023-21117, CVE-2023-21118, CVE-2023-21665, CVE-2023-21666, CVE-2023-26085

Zasiahnuté systémy

Google Android vo verzii bezpečnostných záplat pred 2023-05-05

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 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://source.android.com/docs/security/bulletin/2023-05-01
https://nvd.nist.gov/vuln/detail/CVE-2023-0266

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

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti jadra operačného systému Linux.
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.

Dátum prvého zverejnenia varovania

08.05.2023

CVE

CVE-2023-32233

Zasiahnuté systémy

Linux vo verzii staršej ako 6.3.1 (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. Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať. Detailné inštrukcie môžete nájsť na webovej adrese:
https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=c1592a89942e9678f7d9c8030efa777c0d57edab.
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/254654
https://seclists.org/oss-sec/2023/q2/133

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

Identifikátor

Cisco IOS XE Software IOx Application - bezpečnostná zraniteľnosť

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na IOx hosting systém IOS XE Softvéru, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégiá a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

08.05.2023

CVE

CVE-2023-20065

Zasiahnuté systémy

IOS XE vo verzii staršej ako 17.9.3
Zraniteľnosť Vášho systému možete overiť pomocou online nástroja dostupného na webovej stránke výrobcu:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk#fs

Následky

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

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://github.com/orangecertcc/security-research/security/advisories/GHSA-qrpq-fp26-7v9r
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-priv-escalate-Xg8zkyPk

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

Identifikátor

FRRouting (Border Gateway Protocol) - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu FRRouting.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom špeciálne vytvorenej BGP OPEN správy spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

02.05.2023

CVE

CVE-2022-40302, CVE-2022-40318, CVE-2022-43681

Zasiahnuté systémy

FRRouting vo verzii staršej ako 8.4 (vrátane)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.forescout.com/resources/analyzing-the-security-of-bgp-message-parsing/
https://www.forescout.com/blog/three-new-bgp-message-parsing-vulnerabilities-disclosed-in-frrouting-software/
https://thehackernews.com/2023/05/researchers-uncover-new-bgp-flaws-in.html
https://nvd.nist.gov/vuln/detail/cve-2022-40302

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

Identifikátor

Tenda N301 - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach routra Tenda N301.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k citlivým údajom.
Na uvedené zraniteľnosti je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

03.05.2023

CVE

CVE-2023-29680, CVE-2023-29681

Zasiahnuté systémy

Tenda N301 s firmvérom vo verzii staršej ako 12.02.01.61_multi (vrátane)

Následky

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.
V prípade, že bude pre dané zariadenie ohlásené ukončenie podpory, odporúčame prejsť na iný produkt s platnou podporou.

Zdroje

https://medium.com/@0ta/tenda-n301-v6-cve-2023-29680-cve-2023-29681-a40f7ae6dc62
https://www.redpacketsecurity.com/tenda-n301-devices-information-disclosure-cve-2023-29681/
https://www.redpacketsecurity.com/tenda-n301-devices-information-disclosure-cve-2023-29680/