BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 03. 2023 - 04. 04. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	WordPress Elementor Pro plugin - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Cisco produkty - tri bezpečnostné zraniteľnosti	Vysoká	**8.8**
03.	Google Android - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	TP-Link AX1800 - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Apple produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.6**
06.	NVIDIA produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.4**
07.	Apache James Mail Server - bezpečnostná zraniteľnosť	Vysoká	**8.4**
08.	matrix-js-sdk - bezpečnostná zraniteľnosť	Vysoká	**8.2**
09.	X.org Xserver - bezpečnostná zraniteľnosť	Vysoká	**7.8**
10.	Linux Kernel - bezpečnostná zraniteľnosť	Vysoká	**7.8**
11.	PDF-XChange Editor - bezpečnostná zraniteľnosť	Vysoká	**7.8**
12.	Samba - viacero bezpečnostných zraniteľností	Vysoká	**7.7**
13.	IEEE 802.11 - bezpečnostná zraniteľnosť	Vysoká	**7.5**

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-1085

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

Identifikátor

WordPress Elementor Pro plugin - bezpečnostná zraniteľnosť

Popis

Spoločnosť Elementor vydala bezpečnostnú aktualizáciu na svoj WordPress plugin Elementor Pro, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej AJAX požiadavky získať úplnú kontrolu nad systémom.
Uvedená zraniteľnosť je v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

18.03.2023

CVE

-

IOC

IP adresy aktívne zneužívajúce zraniteľnosť:
193.169.194[.]63
193.169.195[.]64
194.135.30[.]6

Súbory uploadnuté útočníkom:
wp-resortpack.zip
wp-rate.php
lll.zip

Zasiahnuté systémy

Elementor Pro (WordPress plugin) vo verzii staršej ako 3.11.7

Následky

Eskalácia privilégií
Získanie úplnej kontroly nad systémom

Odporúčania
Odporúčame uistiť sa, či Vaše webové stránky založené na redakčnom systéme Wordpress nevyužívajú predmetný plugin v zraniteľnej verzii. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Rovnako odporúčame preveriť a blokovať komunikáciu s IOC v rámci sieťových a bezpečnostných prvkov a preveriť či na súborovom systéme neboli vytvorené súbory s názvami špecifikovanými v časti IOC. Po odstránení zraniteľností, ktoré mohli spôsobiť získanie úplnej kontroly nad systémom 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://thehackernews.com/2023/04/hackers-exploiting-wordpress-elementor.html https://securityaffairs.com/144290/hacking/elementor-pro-wordpress-plugin-critical-bug.html https://patchstack.com/database/vulnerability/elementor-pro/wordpress-elementor-pro-3-11-6-authenticated-arbitrary-options-change-vulnerability https://patchstack.com/articles/critical-elementor-pro-vulnerability-exploited/

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

Identifikátor

Cisco produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktoré opravujú tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa vo webovom manažmentovom rozhraní Cisco Application Policy Infrastructure Controller (APIC) a Cisco Cloud Network Controller spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať CSRF (Cross Site Request Forgery) útok a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti zasiahnutých systémov.

Dátum prvého zverejnenia varovania

29.03.2023

CVE

CVE-2022-20797, CVE-2023-20011, CVE-2023-20113

Zasiahnuté systémy

Cisco APIC vo verzii staršej ako 6.0 (2h)
Cisco Cloud Network Controller vo verzii staršej ako 26.0
Cisco Secure Network Analytics vo verzii staršej ako 7.4.1 (vrátane)
Cisco SD-WAN Software vo verzii staršej ako 20.6.5
Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v sekcii ZDROJE

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému
Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom alebo vykonanie neoprávnených zmien v systéme 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-csrfv-DMx6KSwV
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-2hYb9KFK
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-csrf-76RDbLEh

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
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 69 bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v System komponente spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému. Zneužitie zraniteľnosti nevyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

04.04.2023

CVE

CVE-2021-0872, CVE-2021-0873, CVE-2021-0874, CVE-2021-0875, CVE-2021-0876, CVE-2021-0878, CVE-2021-0879, CVE-2021-0880, CVE-2021-0881, CVE-2021-0882, CVE-2021-0883, CVE-2021-0884, CVE-2021-0885, CVE-2022-20463, CVE-2022-20471, CVE-2022-32599, CVE-2022-33231, CVE-2022-33269, CVE-2022-33270, CVE-2022-33288, CVE-2022-33289, CVE-2022-33302, CVE-2022-33917, CVE-2022-36449, CVE-2022-38181, CVE-2022-40503, CVE-2022-40532, CVE-2022-41757, CVE-2022-42716, CVE-2022-4696, CVE-2022-47335, CVE-2022-47336, CVE-2022-47337, CVE-2022-47338, CVE-2023-20652, CVE-2023-20653, CVE-2023-20654, CVE-2023-20655, CVE-2023-20656, CVE-2023-20657, CVE-2023-20909, CVE-2023-20935, CVE-2023-20941, CVE-2023-20950, CVE-2023-20967, CVE-2023-21080, CVE-2023-21081, CVE-2023-21082, CVE-2023-21083, CVE-2023-21084, CVE-2023-21085, CVE-2023-21086, CVE-2023-21087, CVE-2023-21088, CVE-2023-21089, CVE-2023-21090, CVE-2023-21091, CVE-2023-21092, CVE-2023-21093, CVE-2023-21094, CVE-2023-21096, CVE-2023-21097, CVE-2023-21098, CVE-2023-21099, CVE-2023-21100, CVE-2023-21630

Zasiahnuté systémy

Google Android pred patch úrovňou 2023-04-05

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

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

Zdroje

https://source.android.com/docs/security/bulletin/2023-04-01

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

Identifikátor

TP-Link AX1800 - bezpečnostná zraniteľnosť

Popis

Spoločnosť TP-Link vydala bezpečnostnú aktualizáciu na svoj router AX1800, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.03.2023

CVE

CVE-2023-27346

Zasiahnuté systémy

TP-Link AX1800 s firmvérom vo verzii staršej ako 3_230219

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/251719

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.6
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Xcode, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej aplikácie vykonať na hostitelskom operačnom systéme škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.03.2023

CVE

CVE-2022-26702, CVE-2022-43551, CVE-2022-43552, CVE-2023-0049, CVE-2023-0051, CVE-2023-0054, CVE-2023-0288, CVE-2023-0433, CVE-2023-0512, CVE-2023-23494, CVE-2023-23514, CVE-2023-23523, CVE-2023-23525, CVE-2023-23526, CVE-2023-23527, CVE-2023-23528, CVE-2023-23529, CVE-2023-23532, CVE-2023-23533, CVE-2023-23534, CVE-2023-23535, CVE-2023-23537, CVE-2023-23538, CVE-2023-23540, CVE-2023-23541, CVE-2023-23542, CVE-2023-23543, CVE-2023-27928, CVE-2023-27929, CVE-2023-27931, CVE-2023-27932, CVE-2023-27933, CVE-2023-27934, CVE-2023-27935, CVE-2023-27936, CVE-2023-27937, CVE-2023-27941, CVE-2023-27942, CVE-2023-27943, CVE-2023-27944, CVE-2023-27945, CVE-2023-27946, CVE-2023-27949, CVE-2023-27951, CVE-2023-27952, CVE-2023-27953, CVE-2023-27954, CVE-2023-27955, CVE-2023-27956, CVE-2023-27957, CVE-2023-27958, CVE-2023-27959, CVE-2023-27961, CVE-2023-27962, CVE-2023-27963, CVE-2023-27965, CVE-2023-27967, CVE-2023-27968, CVE-2023-27969, CVE-2023-27970, CVE-2023-28178, CVE-2023-28180, CVE-2023-28181, CVE-2023-28182, CVE-2023-28190, CVE-2023-28192, CVE-2023-28194, CVE-2023-28200

Zasiahnuté systémy

Apple Xcode vo verzii staršej ako 14.3
GarageBand pre macOS vo verzii staršej ako 10.4.8
macOS Ventura vo verzii staršej ako 13.3
macOS Monterey vo verzii staršej ako 12.6.4
macOS Big Sur vo verzii staršej ako 11.7.5
tvOS vo verzii staršej ako 16.4
watchOS vo verzii staršej ako 9.4
iOS 16.4 a iPadOS vo verzii staršej ako 16.4
iOS 15.7.4 a iPadOS vo verzii staršej ako 15.7.4
Safari vo verzii staršej ako 16.4
Studio Display Firmware Update vo verzii staršej ako 16.4

Následky

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

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

Zdroje
https://support.apple.com/en-us/HT213679
https://support.apple.com/en-us/HT213650
https://support.apple.com/en-us/HT213670
https://support.apple.com/en-us/HT213677
https://support.apple.com/en-us/HT213675
https://support.apple.com/en-us/HT213674
https://support.apple.com/en-us/HT213678
https://support.apple.com/en-us/HT213676
https://support.apple.com/en-us/HT213673
https://support.apple.com/en-us/HT213671
https://support.apple.com/en-us/HT213672

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

Identifikátor

NVIDIA produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v NVIDIA DCGM pre Linux spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa spôsobiť zneprístupnenie služby alebo vykonanie neoprávnených zmien v systéme.
Zraniteľnosti vo firmwari systémov NVIDIA DGX by lokálny autentifikovaný útočník mohol zneužiť na vykonanie škodlivého kódu, zneprístupnenie služby, eskaláciu privilégií a vykonanie neoprávnených zmien v systéme.

Dátum prvého zverejnenia varovania

31.03.2023

CVE

CVE-2022-42274, CVE-2022-42280, CVE-2022-42282, CVE-2022-42283, CVE-2022-42286, CVE-2022-42287, CVE-2022-42289, CVE-2022-42290, CVE-2023-0200, CVE-2023-0201, CVE-2023-0202, CVE-2023-0206, CVE-2023-0207, CVE-2023-0208

Zasiahnuté systémy

DCGM pre Linux vo verziách starších ako 3.1.7
DGX-2 BMC vo verziách starších ako 1.08.00
DGX-2 SBIOS vo verziách starších ako 0.33
DGX Station A100 SBIOS vo verziách starších ako 1.18
DGX Station A100 BMC vo verziách starších ako 2.01.00

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Bezpečnostná záplata je obsiahnutá v aktualizácii UEFI BIOS, preto používateľom odporúčame nainštalovať aktualizácie systému UEFI BIOS z webových stránok výrobcu pre ich konkrétne elektronické zariadenie.

Zdroje
https://nvidia.custhelp.com/app/answers/detail/a_id/5453 https://nvidia.custhelp.com/app/answers/detail/a_id/5449 https://exchange.xforce.ibmcloud.com/vulnerabilities/251663

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

Identifikátor

Apache James Mail Server - bezpečnostná zraniteľnosť

Popis

Vývojári mail serveru Apache James vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

31.03.2023

CVE

CVE-2023-26269

Zasiahnuté systémy

James Server vo verzii staršej ako 3.7.4

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/251561

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

matrix-js-sdk - bezpečnostná zraniteľnosť

Popis

Vývojári decentralizačnej komunikačnej platformy matrix.org vydali aktualizáciu svojho JavaScript SDK s názvom matrix-js-sdk, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorených dát spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.03.2023

CVE

CVE-2023-28427

Zasiahnuté systémy

matrix-js-sdk vo verzii staršej ako 24.0.0

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše aplikácie a služby nevyužívajú predmetné SDK v zraniteľnej verzii. V prípade, že áno odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/matrix-org/matrix-js-sdk/security/advisories/GHSA-mwq8-fjpf-c2gr

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

Identifikátor

X.org Xserver - bezpečnostná zraniteľnosť

Popis

Vývojári open source implementácie X Window System servera Xserver vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

29.03.2023

CVE

CVE-2023-1393

Zasiahnuté systémy

xorg-server vo verzii staršej ako 21.1.8

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://lists.x.org/archives/xorg/2023-March/061312.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/251382

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 nachádzajúca sa vo funkcii hci_conn_cleanup funkcii Bluetooth subsystému spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.03.2023

CVE

CVE-2023-28464

Zasiahnuté systémy

Linux Kernel vo verzii staršej ako 6.3.0-rc5

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

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

Zdroje

https://seclists.org/oss-sec/2023/q1/200
https://exchange.xforce.ibmcloud.com/vulnerabilities/251275
https://syzkaller.appspot.com/bug?id=1bb51491ca5df96a5f724899d1dbb87afda61419

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

Identifikátor

PDF-XChange Editor - bezpečnostná zraniteľnosť

Popis

Spoločnosť Tracker Software vydala bezpečnostnú aktualizáciu na svoj produkt PDF-XChange Editor, ktorá opravuje bezpečnostnú zraniteľnosť.
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. Zneužitie zraniteľnosti vyžaduje interakciu používateľa.

Dátum prvého zverejnenia varovania

31.03.2023

CVE

CVE-2023-27345

Zasiahnuté systémy

PDF-XChange Editor vo verzii staršej ako 9.5.367.0

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://exchange.xforce.ibmcloud.com/vulnerabilities/251723
https://www.zerodayinitiative.com/advisories/ZDI-23-357/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.7**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Samba - viacero bezpečnostných zraniteľností

Popis

Vývojári balíka Samba vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje 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.

Dátum prvého zverejnenia varovania

31.03.2023

CVE

CVE-2018-10919, CVE-2022-32743, CVE-2023-0225, CVE-2023-0614, CVE-2023-0922

Zasiahnuté systémy

Samba vo verzii staršej ako 4.6.16, 4.7.9, 4.8.4 a 4.9.7

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://www.samba.org/samba/security/CVE-2023-0225.html
https://www.samba.org/samba/security/CVE-2023-0922.html
https://www.samba.org/samba/security/CVE-2023-0614.html

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

Identifikátor

IEEE 802.11 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o závažnej bezpečnostnej zraniteľnosti vo Wi-Fi sieťach IEEE 802.11. Bezpečnostná zraniteľnosť je založená na nedostatočnej implementácii mechanizmov autentifikácie a umožňuje útočníkov nachádzajúcemu sa v rovnakom sieťovom segmente získať neoprávnený prístup k obsahu komunikácie obete tým, že ju odpojí od access pointu a pripojí sa k nemu s jeho MAC adresou. Útok funguje rovnako úspešne v sieťach so šifrovaním WPA1, WPA2 aj WPA3.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

27.03.2023

CVE

CVE-2022-47522

Zasiahnuté systémy

Všetky systémy využívajúve Wi-Fi siete 802.11

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Vzhľadom na to, že na danú zraniteľnosť neexistuje bezpečnostná záplata odporúčame zraniteľnosť mitigovať podľa odporúčaní od bezpečnostných výskumníkov, detailné inštrukcie môžete nájsť na webovej adrese:
URL v sekcii "Possible mitigations".

Zdroje

https://papers.mathyvanhoef.com/usenix2023-wifi.pdf
https://github.com/vanhoefm/macstealer
https://www.news.de/technik/856818942/ieee-802-11-wlan-gefaehrdet-it-sicherheitswarnung-vom-bsi-und-bug-report-betroffene-systeme-und-produkte-neue-versionen-und-updates-fuer-cve-2022-47522/1/
https://exchange.xforce.ibmcloud.com/vulnerabilities/251520

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-1085