BEZPEČNOSTNÝ BULLETIN

Týždeň 17. 01. 2024 - 23. 01. 2024

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
02.	PAX POS zariadenia - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
03.	Apple - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Mozilla produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
05.	APsystems ECU-C Power Control Software - bezpečnostná zraniteľnosť	Vysoká	**8.8**
06.	NetScaler ADC a NetScaler Gateway - bezpečnostné zraniteľnosti	Vysoká	**8.2**
07.	Dahua produkty - dve bezpečnostné zraniteľnosti	Vysoká	**8.1**
08.	Westermo Lynx 206-F2G - viacero bezpečnostných zraniteľností	Vysoká	**8.0**
09.	AVEVA PI Server - dve bezpečnostné zraniteľnosti	Vysoká	**7.5**
10.	GitHub Enterprise Server - dve bezpečnostné zraniteľnosti	Vysoká	**7.2**
11.	NVIDIA Bluefield 2 a Bluefield 3 DPU BMC - bezpečnostná zraniteľnosť	Vysoká	**7.2**
12.	Progress MOVEit Transfer - bezpečnostná zraniteľnosť	Vysoká	**7.1**
13.	Orthanc Osimis Web Viewer - bezpečnostná zraniteľnosť	Vysoká	**7.1**
14.	Drupal core - bezpečnostná zraniteľnosť	Stredná	**6.5**
15.	GPU od Apple, Qualcomm, AMD a Imagination - bezpečnostná zraniteľnosť	Stredná	**6.5**
16.	Lantronix XPort - bezpečnostná zraniteľnosť	Stredná	**5.7**
17.	SEW-EURODRIVE MOVITOOLS MotionStudio - bezpečnostná zraniteľnosť	Stredná	**5.5**
18.	Integration Objects OPC UA Server Toolkit - bezpečnostná zraniteľnosť	Stredná	**5.3**

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-1491

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

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj internetový prehliadač Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšie bezpečnostné zraniteľnosti nachádzajúce sa v komponente V8 spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú 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

23.01.2024

CVE

CVE-2024-0517, CVE-2024-0518, CVE-2024-0519, CVE-2024-0804, CVE-2024-0805, CVE-2024-0806, CVE-2024-0807, CVE-2024-0808, CVE-2024-0809, CVE-2024-0810, CVE-2024-0811, CVE-2024-0812, CVE-2024-0813, CVE-2024-0814

Zasiahnuté systémy

Chrome pre Mac vo verzii staršej ako 121.0.6167.85
Chrome pre Linux vo verzii staršej ako 121.0.6167.85
Chrome pre Windows vo verzii staršej ako 121.0.6167.85/.86

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/2024/01/stable-channel-update-for-desktop_16.html
https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_23.html

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

Identifikátor

PAX POS zariadenia - viacero bezpečnostných zraniteľností

Popis

Spoločnosť PAX Technology vydala bezpečnostné aktualizácie na svoje platobné terminály, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom injekcie špeciálne upravených príkazov eskalovať svoje privilégiá a následne získať úplnú kontrolu nad systémom.

Dátum prvého zverejnenia varovania

15.01.2024

CVE

CVE-2023-42133, CVE-2023-42134, CVE-2023-42135, CVE-2023-42136, CVE-2023-42137, CVE-2023-4818

Zasiahnuté systémy

PAX A920 zariadenia
PAX A920Pro/A50 zariadenia
PAX Android POS zariadenia s PayDroid

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

Následky

Eskalácia privilégií
Vykonanie škodlivého kódu
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://blog.stmcyber.com/pax-pos-cves-2023/
https://cert.pl/en/posts/2024/01/CVE-2023-4818/

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

Identifikátor

Apple - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2024-23222 sa nachádza v komponente WebKit 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.
Spoločnosť Apple taktiež informovala, že daná kritická bezpečnostná zraniteľnosť môže byť v súčasnosti aktívne zneužívaná útočníkmi.

Dátum prvého zverejnenia varovania

22.01.2024

CVE

CVE-2023-38039, CVE-2023-38545, CVE-2023-38546, CVE-2023-40528, CVE-2023-42887, CVE-2023-42888, CVE-2023-42915, CVE-2023-42916, CVE-2023-42917, CVE-2023-42935, CVE-2023-42937, CVE-2024-23203, CVE-2024-23204, CVE-2024-23206, CVE-2024-23207, CVE-2024-23208, CVE-2024-23209, CVE-2024-23210, CVE-2024-23211, CVE-2024-23212, CVE-2024-23213, CVE-2024-23214, CVE-2024-23215, CVE-2024-23217, CVE-2024-23218, CVE-2024-23219, CVE-2024-23222, CVE-2024-23223, CVE-2024-23224

Zasiahnuté systémy

tvOS vo verzii staršej ako 17.3
watchOS vo verzii staršej ako 10.3
macOS Monterey vo verzii staršej ako 12.7.3
macOS Ventura vo verzii staršej ako 13.6.4
macOS Sonoma vo verzii staršej ako 14.3
iOS vo verzii staršej ako 15.8.1, 16.7.5 a 17.3
iPadOS vo verzii staršej ako 15.8.1, 16.7.5 a 17.3
Safari vo verzii staršej ako 17.3

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
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. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje
https://support.apple.com/en-us/HT214055
https://support.apple.com/en-us/HT214060
https://support.apple.com/en-us/HT214057
https://support.apple.com/en-us/HT214058
https://support.apple.com/en-us/HT214061
https://support.apple.com/en-us/HT214062
https://support.apple.com/en-us/HT214063
https://support.apple.com/en-us/HT214059
https://support.apple.com/en-us/HT214056

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 vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.

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.

Ostatné zraniteľnosi možno zneužiť na zneprístupnenie služby alebo získanie neoprávneného prístupu k citlivým údajom.

Dátum prvého zverejnenia varovania

23.01.2024

CVE

CVE-2024-0741, CVE-2024-0742, CVE-2024-0743, CVE-2024-0744, CVE-2024-0745, CVE-2024-0746, CVE-2024-0747, CVE-2024-0748, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0752, CVE-2024-0753, CVE-2024-0754, CVE-2024-0755

Zasiahnuté systémy

Firefox vo verzii staršej ako 122

Thunderbird vo verzii staršej ako 115.7

Firefox ESR vo verzii staršej ako 115.7

Následky

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

Zneprístupnenie služby

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.

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/280262
https://www.mozilla.org/en-US/security/advisories/mfsa2024-01/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-02/
https://www.mozilla.org/en-US/security/advisories/mfsa2024-04/

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

Identifikátor

APsystems ECU-C Power Control Software - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu ECU-C Power Control Software. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov 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

23.01.2024

CVE

CVE-2022-44037

Zasiahnuté systémy

Energy Communication Unit Power Control Software vo verzii staršej ako C1.2.2 (vrátane)
Energy Communication Unit Power Control Software vo verzii staršej ako v3.11.4 (vrátane)
Energy Communication Unit Power Control Software vo verzii staršej ako W2.1.NA (vrátane)
Energy Communication Unit Power Control Software vo verzii staršej ako v4.1SAA (vrátane)
Energy Communication Unit Power Control Software vo verzii staršej ako v4.1NA (vrátane)

Následky

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

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame sledovať stránky výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-023-01

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

Identifikátor

NetScaler ADC a NetScaler Gateway - bezpečnostné zraniteľnosti

Popis

Spoločnosť Citrix vydala bezpečnostné aktualizácie na produkty NetScaler ADC a Gateway, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2023-6549 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom pretečenia zásobníka vykonať neoprávnené zmeny v systéme a zneprístupnenie služby. Zraniteľnosť je možné zneužiť ak sú zariadenia konfigurované ako gateway (VPN virtuálny server, ICA proxy, CVPN, RDP proxy) alebo AAA virtuálny server.
Zraniteľnosti sú v súčasnosti aktívne zneužívané útočníkmi.

Dátum prvého zverejnenia varovania

19.01.2024

CVE

CVE-2023-6548, CVE-2023-6549

Zasiahnuté systémy

NetScaler ADC a NetScaler Gateway vo verzii staršej ako 14.1-12.35
NetScaler ADC a NetScaler Gateway vo verzii staršej ako 13.1-51.15
NetScaler ADC a NetScaler Gateway vo verzii staršej ako 13.0-92.21
NetScaler ADC vo verzii staršej ako 13.1-FIPS 13.1-37.176
NetScaler ADC vo verzii staršej ako 12.1-FIPS 12.1-55.302
NetScaler ADC vo verzii staršej ako 12.1-NDcPP 12.1-55.302

Následky

Vykonanie škodlivého kódu
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549
https://www.netscaler.com/blog/news/high-severity-updates-are-available-for-netscaler-adc-and-netscaler-gateway/

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

Identifikátor

Dahua produkty - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Dahua Technologies vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov obísť mechanizmy autentifikácie, získať neoprávnený prístup do systému a následne spôsobiť úplné narušenie jeho dôvernosti, itegrity a dostupnosti.

Dátum prvého zverejnenia varovania

18.01.2024

CVE

CVE-2021-33044, CVE-2021-33045

Zasiahnuté systémy

IPC-HX1XXX, HX2XXX, HX3XXX, HX5(4)(3)XXX, HX5XXX, HUM7XXX, HX8XXX
VTO75X95X, VTO65XXX
DHI-ASI7213Y-V3-T1
VTH542XH
PTZ Dome Camera SD1A1, SD22, SD49, SD50, SD52C, SD6AL
Thermal TPC-BF1241, TPC-BF2221, TPC-SD2221, TPC-BF5XXX, PC-SD8X21, TPC-PT8X21B

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE

Následky

Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

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

Zdroje

https://www.dahuasecurity.com/aboutUs/trustedCenter/details/582
http://jvn.jp/en/jp/JVN83655695/index.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.0**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Westermo Lynx 206-F2G - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu Lynx 206-F2G.
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.

Dátum prvého zverejnenia varovania

23.01.2024

CVE

CVE-2023-38579, CVE-2023-40143, CVE-2023-40544, CVE-2023-42765, CVE-2023-45213, CVE-2023-45222, CVE-2023-45227, CVE-2023-45735

Zasiahnuté systémy

Lynx 206-F2G vo verzii firmvéru staršej ako 4.24 (vrátane)

Následky

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

Odporúčania

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

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-023-04

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

Identifikátor

AVEVA PI Server - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť AVEVA vydala bezpečnostnú aktualizáciu na svoj produkt PI Server, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia 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

18.01.2024

CVE

CVE-2023-31274, CVE-2023-34348

Zasiahnuté systémy

AVEVA PI Server vo verzii staršej ako 2018 SP3 Patch 6
AVEVA PI Server vo verzii staršej ako 2023 Patch 1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.aveva.com/content/dam/aveva/documents/support/cyber-security-updates/Security_Bulletin_AVEVA-2024-001.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-24-018-01

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

Identifikátor

GitHub Enterprise Server - dve bezpečnostné zraniteľnosti

Popis

Vývojári platformy GitHub Enterprise Server 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 administrátora prostredníctvom zaslania špeciálne vytvorených DLL súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

16.01.2024

CVE

CVE-2024-0200, CVE-2024-0507

Zasiahnuté systémy

GitHub Enterprise Server vo verzii staršej ako 3.11.3

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://docs.github.com/en/enterprise-server@3.11/admin/release-notes
https://github.blog/2024-01-16-rotating-credentials-for-github-com-and-new-ghes-patches/
https://nvd.nist.gov/vuln/detail/CVE-2024-0200
https://nvd.nist.gov/vuln/detail/CVE-2024-0507

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

Identifikátor

NVIDIA Bluefield 2 a Bluefield 3 DPU BMC - bezpečnostná zraniteľnosť

Popis

Spoločnosť NVIDIA vydala bezpečnostné aktualizácie na produkty Bluefield 2 a Bluefield 3 DPU BMC, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť nachádzajúca sa v komponente ipmitools spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.01.2024

CVE

-

Zasiahnuté systémy

NVIDIA Bluefield 2 a Bluefield 3 DPU BMC vo verzii staršej ako LTS: 2.8.2-51 23.10

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://nvidia.custhelp.com/app/answers/detail/a_id/5511
https://www.cybersecurity-help.cz/vdb/SB2024012328

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Progress MOVEit Transfer - bezpečnostná zraniteľnosť

Popis

Spoločnosť Progress vydala bezpečnostnú aktualizáciu na svoj produkt MOVEit Transfer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme a zneprístupnenie služby.

Dátum prvého zverejnenia varovania

17.01.2024

CVE

CVE-2024-0396

Zasiahnuté systémy

MOVEit Transfer vo verzii staršej ako 2023.1.3 (15.1.3)
MOVEit Transfer vo verzii staršej ako 2023.0.8 (15.0.8)
MOVEit Transfer vo verzii staršej ako 2022.1.11 (14.1.11)
MOVEit Transfer vo verzii staršej ako 2022.0.10 (14.0.10)

Následky

Neoprávnená zmena v systéme
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-January-2024
https://exchange.xforce.ibmcloud.com/vulnerabilities/279739

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Orthanc Osimis Web Viewer - bezpečnostná zraniteľnosť

Popis

Spoločnosť Orthanc vydala bezpečnostnú aktualizáciu na svoj produkt Osimis Web Viewer, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi zrealizovať XSS (Cross-Site Scripting) útok a vykonať škodlivý JavaScript kód vo webovom prehliadači obete.

Dátum prvého zverejnenia varovania

23.01.2024

CVE

CVE-2023-7238

Zasiahnuté systémy

Orthanc vo verzii staršej ako 24.1.2

Následky

Vykonanie škodlivého kódu a 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://discourse.orthanc-server.org/t/osimis-web-viewer-1-4-3/4206
https://www.cisa.gov/news-events/ics-medical-advisories/icsma-24-023-01

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

Identifikátor

Drupal core - bezpečnostná zraniteľnosť

Popis

Vývojári frameworku Drupal vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť v module Comment spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky spôsobiť zneprístupnenie služby. Zraniteľnosť v súčasnosti nemá pridelený identifikátor CVE.
Zraniteľnosť je možné zneužiť len na inštaláciách Drupal s aktivovaným modulom Comment.

Dátum prvého zverejnenia varovania

17.01.2024

CVE

-

Zasiahnuté systémy

Drupal 10.2 vo verzii staršej ako 10.2.2.
Drupal 10.1 vo verzii staršej ako 10.1.8.

Následky

Zneprístupnenie služby

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 zasiahnutých systémov.

Zdroje

https://www.drupal.org/sa-core-2024-001

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

Identifikátor

GPU od Apple, Qualcomm, AMD a Imagination - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti grafických procesorov od výrobcov Apple, Qualcomm, AMD a Imagination.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zneužitia špeciálne vytvorenej aplikácie čiastočne obnoviť dáta z lokálnej pamäte GPU a získať tak neoprávnený prístup k citlivým údajom z LLM a ML modelov bežiacich na danej GPU.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

16.01.2024

CVE

CVE-2023-4969

Zasiahnuté systémy

GPU od výrobcov Apple, Qualcomm, AMD a Imagination

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkazoch v časti ZDROJE

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

V prípade, že Váš systém disponuje grafickým procesorom od jedného z menovaných výrobcov odporúčame preveriť, či sa jedná o zraniteľný model. V prípade, že áno, odporúčame overiť dostupnosť bezpečnostných aktualizácií firmvéru a dostupné záplaty nainštalovať. Alternatívne možno za účelom mitigácie zraniteľnosti obmedziť využívanie LLM a ML na predmetných GPU.
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://blog.trailofbits.com/2024/01/16/leftoverlocals-listening-to-llm-responses-through-leaked-gpu-local-memory/
https://nvd.nist.gov/vuln/detail/CVE-2023-4969
https://www.imaginationtech.com/gpu-driver-vulnerabilities/
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-6010.html
https://lore.kernel.org/linux-firmware/20240111114032.126035-1-quic_akhilpo@quicinc.com/T/#u

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Lantronix XPort - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu XPort.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente z hlavičiek webových požiadaviek extrahovať prihlasovacie údaje.

Dátum prvého zverejnenia varovania

22.01.2024

CVE

CVE-2023-7237

Zasiahnuté systémy

xPort vo všetkých verziách

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, výrobca odporúča prejsť na produkt xPort Edge s odolnejším šifrovaním.
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.cisa.gov/news-events/ics-advisories/icsa-24-023-05

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

SEW-EURODRIVE MOVITOOLS MotionStudio - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu MOVITOOLS MotionStudio. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov získať neoprávnený prístup k citlivým informáciám.

Dátum prvého zverejnenia varovania

16.01.2024

CVE

CVE-2023-6926

Zasiahnuté systémy

SEW-EURODRIVE MOVITOOLS MotionStudio vo verzii staršej ako 6.5.0.2 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.
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.
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-24-016-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Integration Objects OPC UA Server Toolkit - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Integration Objects OPC UA Server Toolkit.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

16.01.2024

CVE

CVE-2023-7234

Zasiahnuté systémy

Integration Objects OPC UA Server Toolkit vo všetkých verziách

Následky

Neoprávnená zmena v systéme

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-24-016-02