BEZPEČNOSTNÝ BULLETIN

Týždeň 10. 05. 2023 - 16. 05. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01794/2022/SK-CERT-1141

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

Identifikátor

Intel produkty - viacero bezpečnostných zraniteľností

Popis

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

Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte Intel OFU Software, 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 zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.05.2023

CVE

CVE-2022-21229, CVE-2022-21239, CVE-2022-21804, CVE-2022-25772, CVE-2022-25976, CVE-2022-27180, CVE-2022-28699, CVE-2022-29508, CVE-2022-29919, CVE-2022-30338, CVE-2022-31477, CVE-2022-32576, CVE-2022-32577, CVE-2022-32578, CVE-2022-32582, CVE-2022-32766, CVE-2022-33894, CVE-2022-33963, CVE-2022-34147, CVE-2022-34848, CVE-2022-34855, CVE-2022-36339, CVE-2022-36391, CVE-2022-37327, CVE-2022-37409, CVE-2022-38087, CVE-2022-38101, CVE-2022-38103, CVE-2022-38787, CVE-2022-40207, CVE-2022-40210, CVE-2022-40685, CVE-2022-40972, CVE-2022-40974, CVE-2022-41610, CVE-2022-41621, CVE-2022-41628, CVE-2022-41646, CVE-2022-41658, CVE-2022-41687, CVE-2022-41690, CVE-2022-41693, CVE-2022-41699, CVE-2022-41769, CVE-2022-41771, CVE-2022-41784, CVE-2022-41801, CVE-2022-41808, CVE-2022-41979, CVE-2022-41982, CVE-2022-41998, CVE-2022-42465, CVE-2022-42878, CVE-2022-43465, CVE-2022-43474, CVE-2022-43475, CVE-2022-43507, CVE-2022-44610, CVE-2022-44619, CVE-2022-45128, CVE-2022-46279, CVE-2022-46645, CVE-2022-46656, CVE-2023-22297, CVE-2023-22312, CVE-2023-22355, CVE-2023-22379, CVE-2023-22440, CVE-2023-22442, CVE-2023-22443, CVE-2023-22447, CVE-2023-22661, CVE-2023-23569, CVE-2023-23573, CVE-2023-23580, CVE-2023-23909, CVE-2023-23910, CVE-2023-24475, CVE-2023-25175, CVE-2023-25179, CVE-2023-25545, CVE-2023-25771, CVE-2023-25772, CVE-2023-25776, CVE-2023-27298, CVE-2023-27382, CVE-2023-27386, CVE-2023-28410, CVE-2023-28411

Zasiahnuté systémy

Intel® NUC Chaco Canyon BIOS vo verzii staršej ako iFlashV Windows 5.13.00.2105
Intel® Connect M Android vo verzii staršej ako 1.82
Intel® QAT drivers pre Windows vo verzii staršej ako 1.9.0
Intel® NUC firmware (pre presný zoznam zasiahnutých verzií viď. security advisory 00777)
Intel® DCM software vo verzii staršej ako 5.0.1.
Intel® VTune™ Profiler software vo verzii staršej ako 2023.0.
Intel® oneAPI Base Toolkit vo verzii staršej ako 2023.0.
Intel® System Bring-up Toolkit vo verzii staršej ako 2023.0
Intel® Unite® Plugin SDK vo verzii staršej ako 4.2 or later.
Intel® VROC software vo verzii staršej ako 7.7.6.1003.
Intel® SUR software vo verzii staršej ako 2.4.8989
Intel® MacCPUID software vo verzii staršej ako 3.2.

Intel® Unite® Client software pre Windows vo verzii staršej ako 4.2.34870
Intel® i915 Graphics pre Linux vo verzii staršej ako kernel 6.2.10.
Intel® Pathfinder pre RISC-V vo všetkých verziách (EoL)
Intel® NUC Software Studio Service vo verzii staršej ako 1.17.38.0
WULT software maintained by Intel® vo verzii staršej ako 1.0.0 (commit id 592300b).
Intel® Retail Edge Mobile (IREP) iOS vo verzii staršej ako 3.4.7
Intel® Server Board M50CYP Family BMC firmware vo verzii staršej ako 2.90.
Intel® Server Board D50TNP Family BMC firmware vo verzii staršej ako 2.90.
Intel® NUC Pro Software Suite vo verzii staršej ako 2.0.0.3.
Intel® Retail Edge Mobile (IREP) iOS vo verzii staršej ako 3.4.7
Intel® Retail Edge Mobile android vo verzii staršej ako 3.0.301145-RELEASE
Intel® SCS Add-on software pre Microsoft SCCM vo všetkých verziách (EoL)
Open CAS software pre Linux maintained by Intel vo verzii staršej ako 22.6.2.
Intel® Unite® android application vo verzii staršej ako Release 17
FPGA product families vo verzii staršej ako 2.7.0 HotFix
Intel® Advisor pre oneAPI vo verzii staršej ako 2023.0.
Intel® CPU Runtime pre OpenCL™ Applications vo verzii staršej ako 2023.0.
Intel® Distribution pre Python* programming language vo verzii staršej ako 2023.0.
Intel® DPC++ Compatibility Tool vo verzii staršej ako 2023.0.
Intel® Embree Ray Tracing Kernel Library vo verzii staršej ako 2023.0.
Intel® Fortran Compiler vo verzii staršej ako 2023.0.
Intel® Implicit SPMD Program Compiler vo verzii staršej ako 1.18.1.
Intel® Inspector pre oneAPI vo verzii staršej ako 2023.0.
Intel® Integrated Performance Primitives vo verzii staršej ako 2021.7.
Intel® IPP Cryptography vo verzii staršej ako 2021.6.3.
Intel® MPI Library vo verzii staršej ako 2021.8.
Intel® oneAPI Base Toolkit vo verzii staršej ako 2023.0.
Intel® oneAPI Data Analytics Library vo verzii staršej ako 2023.0.
Intel® oneAPI Deep Neural Network Library vo verzii staršej ako 2023.0.
Intel® oneAPI DPC++/C++ Compiler vo verzii staršej ako 2023.0.
Intel® oneAPI DPC++ Library (oneDPL) vo verzii staršej ako 2022.0.
Intel® oneAPI HPC Toolkit vo verzii staršej ako 2023.0.
Intel® oneAPI IoT Toolkit vo verzii staršej ako 2023.0.
Intel® oneAPI Math Kernel Library vo verzii staršej ako 2023.0.
Intel® oneAPI Rendering Toolkit vo verzii staršej ako 2023.0.
Intel® oneAPI Threading Building Blocks vo verzii staršej ako 2021.8.
Intel® oneAPI Video Processing Library vo verzii staršej ako 2023.0.
Intel® Open Image Denoise vo verzii staršej ako 1.4.3.
Intel® Open Volume Kernel Library vo verzii staršej ako 2023.0.
Intel® OSPRay vo verzii staršej ako 2023.0.
Intel® OSPRay Studio vo verzii staršej ako 2023.0.
Intel® Trace Analyzer and Collector vo verzii staršej ako 2021.8.0.
Intel® VTune™ Profiler pre oneAPI vo verzii staršej ako 2023.0.
DSP Builder software installer vo verzii staršej ako 22.4 pre Intel® FPGAs Pro Edition.
Intel® Smart Campus Android application vo verzii staršej ako 9.9.
The Intel® QAT Driver pre Windows vo verzii staršej ako 1.9.0-0008.
The Intel® QAT Driver pre Linux vo verzii staršej ako 1.7.l.4.12.
Intel® EMA Configuration Tool software vo verzii staršej ako 1.0.4.
Intel® MC software vo verzii staršej ako 2.4.
10th Generation Intel® Core™ Processor Family

7th Generation Intel® Core™ Processor Family
8th Generation Intel® Core™ Processor Family
8th Generation Intel® Core™ Processors
9th Generation Intel® Core™ Processor Family
Intel® Xeon® D processor Family
Intel® Xeon® E Processor Family
Intel® Xeon® Platinum P-8124, P-8136 processors
Intel® Xeon® Processor E Family
Intel® Xeon® Scalable Processor Family
Intel® Xeon® W processor Family
Intel® DCM software vo verzii staršej ako 5.1.
Intel® Trace Analyzer and Collector software vo verzii staršej ako 2021.8.0 publikovanej v Dec 2022.
Intel® oneAPI HPC Toolkit vo verzii staršej ako 2023.0.0.
Audio Install Package pre Windows® 10 pre niektoré Intel® NUC P14E Laptop Element software vo verzii staršej ako 1.0.0.156
HotKey Services pre Windows® 10 pre niektoré Intel® NUC P14E Laptop Element software vo verzii staršej ako 1.1.44
Intel® Quartus® Prime Pro edition software vo verzii staršej ako 22.3.
Intel® QAT Engine pre OpenSSL vo verzii staršej ako 0.6.16.
Intel® EMA software vo verzii staršej ako 1.9.0.0.
Intel® SCS software vo všetkých verziách (EoL)
Intel® OFU software vo verzii staršej ako 14.1.30.
Intel® IPP Cryptography software vo verzii staršej ako 2021.6.

Následky

Eskalácia privilégií

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.intel.com/content/www/us/en/security-center/advisory/intel-sa-00780.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00779.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00778.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00777.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00772.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00771.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00723.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00692.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00785.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00784.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00782.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00886.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00855.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00854.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00853.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00847.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00839.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00834.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00847.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00832.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00827.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00825.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00824.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00819.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00816.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00815.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00809.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00808.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00807.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00806.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00805.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00802.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00799.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00798.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00797.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00796.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00792.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00788.html

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

Identifikátor

VMware Aria Operations - viacero bezpečnostných zraniteľností

Popis

Spoločnosť VMware vydala bezpečnostnú aktualizáciu na svoj produkt Aria Operations, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, 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

11.05.2023

CVE

CVE-2023-20877, CVE-2023-20878, CVE-2023-20879, CVE-2023-20880

Zasiahnuté systémy

VMware Aria Operations vo verzii staršej ako 8.10 Hot Fix 4

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://www.vmware.com/security/advisories/VMSA-2023-0009.html

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

Identifikátor

myREX24, myREX24.virtual a MB connect line - dve bezpečnostné zraniteľnosti

Popis

Spoločnosti Helmholz a MB connect line vydali bezpečnostné aktualizácie na produkty myREX24, myREX24.virtual, mbCONNECT24 a mymbCONNECT24, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa zmeniť heslo ktoréhokoľvek používateľa, získať neoprávnený prístup k citlivým údajom a následne vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.05.2023

CVE

CVE-2023-0985, CVE-2023-1779

Zasiahnuté systémy

mbCONNECT24 vo verzii staršej ako 2.13.4
mymbCONNECT24 vo verzii staršej ako 2.13.4
myREX24 vo verzii staršej ako 2.13.4
myREX24.virtual vo verzii staršej ako 2.13.4

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Výrobca tiež odporúča nastaviť viacfaktorovú autentifikáciu.
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://cert.vde.com/en/advisories/VDE-2023-008/
https://cert.vde.com/en/advisories/VDE-2023-002/

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

Identifikátor

D-Link DIR-2150 - viacero bezpečnostných zraniteľností

Popis

Spoločnosť D-Link vydala bezpečnostnú aktualizáciu na svoj router DIR-2150, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

15.05.2023

CVE

-

Zasiahnuté systémy

D-Link DIR-2150 vo verzii firmvéru staršej ako v1.06

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

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

Zdroje

https://www.zerodayinitiative.com/advisories/ZDI-23-628/
https://www.zerodayinitiative.com/advisories/ZDI-23-631/
https://www.zerodayinitiative.com/advisories/ZDI-23-625/
https://www.zerodayinitiative.com/advisories/ZDI-23-626/
https://www.zerodayinitiative.com/advisories/ZDI-23-627/
https://www.zerodayinitiative.com/advisories/ZDI-23-629/
https://www.zerodayinitiative.com/advisories/ZDI-23-630/

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

Identifikátor

BirdDog Cameras and Encoders - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť BirdDog vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v existencii zabudovaného používateľského účtu s predvoleným heslom a umožňuje lokálnemu, neautentifikovanému útočníkovi eskalovať svoje privilégiá a následne vykonať škodlivý kód na úrovni používateľa root s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

17.05.2023

CVE

CVE-2023-2504, CVE-2023-2505

Zasiahnuté systémy

4K QUAD vo verzii staršej ako 4.5.181 a 4.5.196 (vrátane)
MINI vo verzii staršej ako 2.6.2 (vrátane)
A300 EYES vo verzii staršej ako 3.4 (vrátane)
STUDIO R3 vo verzii staršej ako 3.6.4 (vrátane)

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://www.cisa.gov/news-events/ics-advisories/icsa-23-131-11

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

Identifikátor

PTC Vuforia Studio - viacero bezpečnostných zraniteľností

Popis

Spoločnosť PTC vydala bezpečnostnú aktualizáciu na svoj produkt Vuforia Studio, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.05.2023

CVE

CVE-2023-24476, CVE-2023-27881, CVE-2023-29152, CVE-2023-29168, CVE-2023-29502, CVE-2023-31200

Zasiahnuté systémy

Vuforia Studio vo verzii staršej ako 9.9

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.cisa.gov/news-events/ics-advisories/icsa-23-131-13

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

Identifikátor

Beekeeper Studio - bezpečnostná zraniteľnosť

Popis

Vývojári klienta Beekeeper Studio 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 injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

12.05.2023

CVE

CVE-2023-28394

Zasiahnuté systémy

Beekeeper Studio vo verzii staršej ako 3.9.9

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

http://jvn.jp/en/jp/JVN11705010/index.html

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

Identifikátor

Adobe Substance 3D Painter - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Adobe vydala bezpečnostnú aktualizáciu na svoj produkt Substance 3D Painter, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.05.2023

CVE

CVE-2023-29273, CVE-2023-29274, CVE-2023-29275, CVE-2023-29276, CVE-2023-29277, CVE-2023-29278, CVE-2023-29279, CVE-2023-29280, CVE-2023-29281, CVE-2023-29282, CVE-2023-29283, CVE-2023-29284, CVE-2023-29285, CVE-2023-29286

Zasiahnuté systémy

Adobe Substance 3D Painter vo verzii staršej ako 8.3.1

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://helpx.adobe.com/security/products/substance3d_painter/apsb23-29.html

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

Identifikátor

Lenovo ThinkPad Dock Firmware - bezpečnostná zraniteľnosť

Popis

Spoločnosť Lenovo vydala bezpečnostnú aktualizáciu firmvéru pre ThinkPad Dock, 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 vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.05.2023

CVE

CVE-2022-4569

Zasiahnuté systémy

ThinkPad Dock Firmware Udpate Tool vo verzii staršej ako v1.0.35_v2

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://exchange.xforce.ibmcloud.com/vulnerabilities/254973
https://support.lenovo.com/us/en/product_security/LEN-103544

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

Identifikátor

AMD EPYC Processors - viacero bezpečnostných zraniteľností

Popis

Spoločnosť AMD vydala bezpečnostnú aktualizáciu na svoje portfólio produktov, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

09.05.2023

CVE

CVE-2021-26354, CVE-2021-26356, CVE-2021-26371, CVE-2021-26379, CVE-2021-26397, CVE-2021-26406, CVE-2021-46755, CVE-2021-46756, CVE-2021-46762, CVE-2021-46763, CVE-2021-46764, CVE-2021-46769, CVE-2021-46775, CVE-2022-23818, CVE-2023-20520, CVE-2023-20524

Zasiahnuté systémy

1st Gen AMD EPYC™ Processors vo verzii staršej ako NaplesPI 1.0.0.J
2nd Gen AMD EPYC™ Processors vo verzii staršej ako RomePI 1.0.0.E
3rd Gen AMD EPYC™ Processors vo verzii staršej ako MilanPI 1.0.0.9
4th Gen AMD EPYC™ Processors vo verzii staršej ako "Genoa"

Následky

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

Odporúčania

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

Zdroje

https://www.amd.com/en/resources/product-security/bulletin/amd-sb-3001.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/255100

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

Identifikátor

Mozilla Thunderbird - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mozilla Foundation vydala bezpečnostnú aktualizáciu na svoj produkt Thunderbird, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

09.05.2023

CVE

CVE-2023-32205, CVE-2023-32206, CVE-2023-32207, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32214, CVE-2023-32215

Zasiahnuté systémy

Thunderbird vo verzii staršej ako 102.11

Následky

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 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.mozilla.org/en-US/security/advisories/mfsa2023-18/
https://access.redhat.com/security/cve/cve-2023-32205

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

Identifikátor

OpenStack Cinder, Glance_store, Nova and Os-brick - bezpečnostná zraniteľnosť

Popis

Vývojári OpenStack vydali bezpečnostné aktualizácie svojich produktov, ktoré opravujú bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

10.05.2023

CVE

CVE-2023-2088

Zasiahnuté systémy

Cinder vo verzii staršej ako 20.2.1 a 21.2.1
Glance_store vo verzii staršej ako 3.0.1, 4.1.1, a 4.3.1
Nova vo verzii staršej ako 25.1.2 a 26.1.2
Os-brick vo verzii staršej ako 5.2.3, 6.1.1 a 6.2.2

Následky

Neoprávnený prístup k citlivým údajom

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/254976
https://seclists.org/oss-sec/2023/q2/140

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

Identifikátor

HPE StoreOnce - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť Hewlett Packard Enterprise vydala bezpečnostnú aktualizáciu na svoj produkt StoreOnce, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi s fyzickým prístupom k zariadeniu eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť znepristupnenie služby.

Dátum prvého zverejnenia varovania

16.05.2023

CVE

CVE-2021-0060, CVE-2021-0147, CVE-2021-33068

Zasiahnuté systémy

HPE StoreOnce 3620 vo verzii staršej ako SPS_E5_04.01.04.601
HPE StoreOnce 3640 vo verzii staršej ako SPS_E5_04.01.04.601
HPE StoreOnce 5200 vo verzii staršej ako SPS_E5_04.01.04.601
HPE StoreOnce 5250 vo verzii staršej ako SPS_E5_04.01.04.601
HPE StoreOnce 5650 vo verzii staršej ako SPS_E5_04.01.04.601

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://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04242en_us