ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits d'Intel
Numéro de Référence	43291008/23
Date de publication	10 Aout 2023
Risque	Important
Impact	Important

Systèmes affectés

- Intel Support versions antérieures à la version v23.02.07
- Intel Unite versions antérieures à la version 4.2.3504
- NUC sans les correctifs de sécurité du 08 août 2023
- Hyperscan versions antérieures à la version 5.4.1
- Intel Arc A770 et A750 vendues entre octobre 2022 et décembre 2022
- Intel Unite pour Mac versions antérieures à la version 4.2.11
- OpenVINO versions antérieures à la version 2022.3.0
- Intel Unite pour Windows versions antérieures à la version 4.2.34962
- Intel Active Management Technology (AMT) sans les correctifs de sécurité du 08 août 2023
- Intel BIOS PCSD BIOS versions antérieures à la version 02.01.0013
- Intel Converged Security Management Engine (CSME) sans les correctifs de sécurité du 08 août 2023
- Intel SSD Tools software versions antérieures à la version mdadm-4.2-rc2
- Intel Standard Manageability software sans les correctifs de sécurité du 08 août 2023
- Intel PROSet/Wireless WiFi versions antérieures à la version 22.200
- Interface utilisateur Intel RST et pilotes versions antérieures à la version 16.8.5.1014.5
- Intel AI Hackathon versions antérieures à la version 2.0.0
- Intel Agilex software inclus dans Intel Quartus Prime Pro Edition pour Linux versions antérieures à la version 22.4
- Intel DSA versions antérieures à la version 23.1.9
- Intel DTT versions antérieures à la version 8.7.10801.25109
- Intel Easy Streaming Wizard toutes versions [1]
- Intel ITS versions antérieures à la version 3.1
- Intel Manageability Commander versions antérieures à la version 2.3

- Intel Optimization for TensorFlow versions antérieures à la version 2.12
- Intel PROSet/Wireless WiFi 6 AX200 sur certaines plateformes Microsoft Surface versions antérieures à la version 22.220 HF
- Intel RealSense ID pour Intel RealSense 450 FA versions antérieures à la version 0.25
- Intel SDP Tool versions antérieures à la version 1.4 build 5
- Intel Unison versions antérieures à la version 10.12
- Intel oneMKL versions antérieures à la version 2022.0
- MAVinci Desktop pour Intel Falcon 8+ toutes versions [2]
- Intel oneVPL GPU versions antérieures à la version 22.6.5
- Intel ISPC software pour Windows versions antérieures à la version 1.19.0
- Intel Advanced Link Analyzer Standard Edition versions antérieures à la version 22.1.1
- Intel VCUST téléchargés avant le 03 février 2023 sans le correctif de sécurité du 08 août 2023
- Intel oneAPI versions antérieures à la version 2023.1.0
- Intel PSR versions antérieures à la version 1.0.0.20
- Intel RealSense versions antérieures à la version 2.53.1
- Pilote RDMA des Contrôleurs Ethernet Intel pour linux versions antérieures à la version 1.9.30
- Pilotes infrarouge ITE Tech consumer pour terminaux NUC versions antérieures à la version 5.5.2.1
- Pilotes vidéo BMC intégrés aux cartes mères Intel M10JNP2SB pour Linux versions antérieures à la version 1.13.4
- Pilotes vidéo BMC intégrés aux cartes mères Intel M10JNP2SB pour Microsoft versions antérieures à la version 3.0
- Intel RST avec Intel Optane Memory (plateformes de 10ème et 11ème générations) versions antérieures à la version 18.7.6.1010.3
- Intel RST avec Intel Optane Memory (plateformes de 11ème à 13ème générations) versions antérieures à la version 19.5.2.1049.5
- Intel RST avec Intel Optane Memory (plateformes de 8ème et 9ème générations) versions antérieures à la version 17.11.3.1010.2
- Intel Quartus Prime Pro pour Linux before versions antérieures à la version 22.4
- Intel Quartus Prime Standard pour Linux versions antérieures à la version 22.1STD
- Intel NUC Pro pour Windows versions antérieures à la version 2.0.0.9
- System Firmware Update Utility (SysFwUpdt) for Intel Server Boards and Intel Server Systems Based on Intel 621A Chipset before version 16.0.7.
- Séries de contrôleurs Ethernet et adaptateurs E810 (Columbiaville) versions antérieures à la version 1.7.2.4
- Séries de processeurs Intel Atom, Xeon, Core de 7ème à 11ème générations, Celeron, Pentium et Core séries X sans les correctifs de sécurité du 08 août 2023
- Séries de processeurs Intel Atom, Xeon, Core, Celeron et Pentium sans les correctifs de sécurité du 08 août 2023
- Utilitaire de mise à jour de microgiciel (SysFwUpdt) pour Intel Server Boards et Intel Server Systems basé sur les jeux de puces 621A
- Intel VROC versions antérieures à la version 8.0.0.4035

Identificateurs externes

CVE-2022-25864 CVE-2022-27635 CVE-2022-27879 CVE-2022-29470 CVE-2022-29871
CVE-2022-29887 CVE-2022-34657 CVE-2022-36351 CVE-2022-36372 CVE-2022-36392
CVE-2022-37336 CVE-2022-37343 CVE-2022-38076 CVE-2022-38083 CVE-2022-38102
CVE-2022-38973 CVE-2022-40964 CVE-2022-40982 CVE-2022-41804 CVE-2022-41984
CVE-2022-43456 CVE-2022-43505 CVE-2022-44611 CVE-2022-44612 CVE-2022-45112
CVE-2022-46329 CVE-2023-22276 CVE-2023-22330 CVE-2023-22338 CVE-2023-22356
CVE-2023-22444 CVE-2023-22449 CVE-2023-22840 CVE-2023-22841 CVE-2023-23577
CVE-2023-23908 CVE-2023-24016 CVE-2023-25182 CVE-2023-25757 CVE-2023-25773
CVE-2023-25775 CVE-2023-25944 CVE-2023-26587 CVE-2023-27391 CVE-2023-27392
CVE-2023-27505 CVE-2023-27506 CVE-2023-27509 CVE-2023-27515 CVE-2023-27887
CVE-2023-28380 CVE-2023-28385 CVE-2023-28405 CVE-2023-28658 CVE-2023-28711
CVE-2023-28714 CVE-2023-28736 CVE-2023-28823 CVE-2023-28938 CVE-2023-29151
CVE-2023-29243 CVE-2023-29494 CVE-2023-29500 CVE-2023-30760 CVE-2023-31246
CVE-2023-32285 CVE-2023-32543 CVE-2023-32547 CVE-2023-32609 CVE-2023-32617
CVE-2023-32656 CVE-2023-32663 CVE-2023-33867 CVE-2023-33877 CVE-2023-34086
CVE-2023-34349 CVE-2023-34355 CVE-2023-34427 CVE-2023-34438

Bilan de la vulnérabilité

Intel annonce la disponibilité de mises à jour de sécurité qui corrigent des vulnérabilités critiques affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d’accéder à des données confidentielles, d’élever ses privilèges ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité d’Intel pour appliquer les correctifs nécessaires

Risque

- Accès à des informations confidentielles.
- Elévation de privilèges.
- Déni de service.

Références

Bulletins de sécurité d'Intel :

- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00690.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00742.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00766.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00783.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00794.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00795.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00800.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00812.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00813.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00818.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00826.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00829.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00830.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00835.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00836.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00837.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00840.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00842.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00844.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00846.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00848.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00849.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00850.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00859.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00862.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00868.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00872.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00873.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma

- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00875.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00877.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00878.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00879.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00890.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00892.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00893.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00897.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00899.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00905.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00907.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00912.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00917.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00932.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00934.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00938.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00946.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma