ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Intel
Numéro de Référence	44891711/23
Date de Publication	17 Novembre 2023
Risque	Important
Impact	Important

Systèmes affectés

- 10ème génération de processeur Intel Core, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- 11ème génération de processeur Intel Core, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- 12ème génération de processeur Intel Core, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- 13ème génération de processeur Intel Core, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- 8ème génération de processeur Intel Core, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- 9ème génération de processeur Intel Core, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- Application Intel Smart Campus pour Android versions antérieures à 9.4
- Application Intel Support pour Android toutes versions
- Bibliothèque Intel QAT Library (QATlib) versions antérieures à 22.07.1
- Intel Advisor versions antérieures à 2023.1
- Intel Arc RGB Controller versions antérieures à 1.06
- Intel Chipset Device versions antérieures à 10.1.19444.8378
- Intel Connectivity Performance Suite sans le dernier correctif de sécurité
- Intel DCM versions antérieures à 5.2
- Intel In-Band Manageability versions antérieures à 3.0.14
- Intel Inspector versions antérieures à 2023.1

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- Intel MPI Library versions antérieures à 2021.9
- Intel OFU versions antérieures à 14.1.31
- Intel On Demand Agent sans le dernier correctif de sécurité
- Intel OpenVINO Model Server versions antérieures à 2022.3
- Intel OpenVINO toolkit versions antérieures à 2023.0.0
- Intel QAT pour Linux versions antérieures à QAT20.L.1.0.40-00004
- Intel Rapid Storage Technology versions antérieures à 16.8.5.1014.9
- Intel RealSense Dynamic Calibration versions antérieures à 2.13.1.0
- Intel Server Configuration Utility versions antérieures à 16.0.9
- Intel Simics Simulator versions antérieures à 1.7.2
- Intel Unison sans le dernier correctif de sécurité
- Intel XTU versions antérieures à 7.12.0.15
- Intel oneAPI Base Toolkit versions antérieures à 2023.1
- Intel oneAPI HPC Toolkit versions antérieures à 2023.1
- Logiciels pour Intel NUC
- Micrologiciel Intel FPGA versions antérieures à 2.8.1
- Micrologiciel Intel NUC, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- Micrologiciels Intel Ethernet Adapters
- Micrologiciels Intel Ethernet Controllers
- Micrologiciels Intel Optane SSD et Intel Optane SSD DC
- Micrologiciels Intel Server Board et Server System
- Outil Intel Battery Life Diagnostic versions antérieures à 2.2.1
- Pilote Intel QAT pour Windows HW versions 1.x antérieures à 1.10
- Pilote Intel QAT pour Windows HW versions 2.x antérieures à 2.04
- Pilote pour Radeon RX Vega M (intégré dans les processeurs Intel Core) versions antérieures à 23.10.01.46
- Pilotes Intel Arc & Iris Xe Graphics WHQL pour Windows versions antérieures à 31.0.101.4255
- Processeur Intel Atom, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- Processeur Intel Celeron, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- Processeur Intel Pentium, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations

- Processeur Intel Server, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- Processeur Intel Xeon D, veuillez-vous référer aux avis de l'éditeur pour plus d'Informations
- Utilitaire Intel Server Information Retrieval versions antérieures à 16.0.9

Identificateurs externes

- CVE-2021-46748 CVE-2022-24379 CVE-2022-27229 CVE-2022-29262 CVE-2022-29510 CVE-2022-33898 CVE-2022-33945 CVE-2022-34301 CVE-2022-34302 CVE-2022-34303 CVE-2022-36374 CVE-2022-36377 CVE-2022-36396 CVE-2022-41659 CVE-2022-41689 CVE-2022-41700 CVE-2022-42879 CVE-2022-43477 CVE-2022-43666 CVE-2022-45109 CVE-2022-45469 CVE-2022-46298 CVE-2022-46299 CVE-2022-46301 CVE-2022-46646 CVE-2022-46647 CVE-2023-20567 CVE-2023-20568 CVE-2023-22285 CVE-2023-22290 CVE-2023-22292 CVE-2023-22305 CVE-2023-22310 CVE-2023-22313 CVE-2023-22327 CVE-2023-22329 CVE-2023-22337 CVE-2023-22448 CVE-2023-22663 CVE-2023-23583 CVE-2023-24587 CVE-2023-24588 CVE-2023-25071 CVE-2023-25075 CVE-2023-25080 CVE-2023-25756 CVE-2023-25949 CVE-2023-25952 CVE-2023-26589 CVE-2023-27305 CVE-2023-27306 CVE-2023-27513 CVE-2023-27519 CVE-2023-27879 CVE-2023-28376 CVE-2023-28377 CVE-2023-28378 CVE-2023-28388 CVE-2023-28397 CVE-2023-28401 CVE-2023-28404 CVE-2023-28723 CVE-2023-28737 CVE-2023-28740 CVE-2023-28741 CVE-2023-29157 CVE-2023-29161 CVE-2023-29165 CVE-2023-29504 CVE-2023-31203 CVE-2023-31273 CVE-2023-32204 CVE-2023-32278 CVE-2023-32279 CVE-2023-32283 CVE-2023-32638 CVE-2023-32641 CVE-2023-32655 CVE-2023-32658 CVE-2023-32660 CVE-2023-32661 CVE-2023-33872 CVE-2023-33874 CVE-2023-33878 CVE-2023-34314 CVE-2023-34350 CVE-2023-34431 CVE-2023-34997 CVE-2023-36860 CVE-2023-38131 CVE-2023-38411 CVE-2023-38570 CVE-2023-39221 CVE-2023-39228 CVE-2023-39230 CVE-2023-39411 CVE-2023-39412 CVE-2023-40220 CVE-2023-40540

Bilan de la vulnérabilité

Intel a publié une mise à jour de sécurité corrigeant plusieurs vulnérabilités recensées dans les produits susmentionnés. L’exploitation de ces vulnérabilités peut permettre à un attaquant de porter atteinte à la confidentialité de données, de contourner la politique de sécurité, de réussir une élévation de privilèges et de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité Intel du 14 Novembre 2023 pour plus d’information.

Risque

- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Elévation de privilèges
- Déni de service

Annexe

Bulletin de sécurité Intel du 14 Novembre 2023:

- https://www.intel.com/content/www/us/en/security-center/default.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma