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	41821105/23
Date de Publication	11 Mai 2023
Risque	Important
Impact	Important

Systèmes affectés

- 2023.2 IPU – BIOS
- DSP Builder pour Intel FPGAs Pro Edition Software
- Intel NUC BIOS Firmware
- Intel Connect M Android App
- Intel DCM Software
- Intel DCM
- Intel EMA Configuration Tool and Intel MC Software
- Intel EMA Software
- Intel FPGA Firmware
- Intel IPP Cryptography
- Intel MacCPUID Software
- Intel NUC BIOS Update Software
- Intel NUC Laptop Element Software
- Intel NUC Pro Software Suite
- Intel NUC Software Studio Service Installer
- Intel OFU Software
- Intel Pathfinder pour RISC-V
- Intel QAT Driver
- Intel QAT Engine pour OpenSSL
- Intel QAT

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 Quartus Prime Pro Software
- Intel Retail Edge Mobile App
- Intel SCS Add-on Software Installer
- Intel SCS Software
- Intel SUR Software
- Intel Server Board BMC Firmware
- Intel Smart Campus Android App
- Intel Trace Analyzer and Collector Software
- Intel Unite Android App
- Intel Unite Client Software
- Intel Unite Plugin SDK
- Intel VROC Software
- Intel VTune™ Profiler
- Intel i915 Graphics Drivers pour Linux
- Intel oneAPI Toolkit and Component Software Installers
- Open CAS
- WULT Software

Identificateurs externes

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

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 09 Mai 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 09 Mai 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