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	40341602/23
Date de Publication	16 Février 2023
Risque	Important
Impact	Important

Systèmes affectés

- Intel oneAPI Toolkits versions antérieures à 2022.2
- Intel oneAPI DPC++/C++ Compiler versions antérieures à 2022.1
- Intel C++ Compiler Classic versions antérieures à 2021.6
- Intel oneapi-cli pour Intel oneAPI Toolkits versions antérieures à 0.2.0
- Intel FPGA Add-on pour Intel oneAPI Toolkits versions antérieures à 2022.2
- Intel Trace Analyzer and Collector versions antérieures à 2021.5
- Intel oneAPI Data Analytics Library versions antérieures à 2021.5
- Intel oneAPI Collective Communications Library (oneCCL) versions antérieures à 2021.6
- Intel Distribution pour le langage de programmation Python versions antérieures à 2022.1
- Intel oneAPI Deep Neural Network (oneDNN) versions antérieures à 2022.1
- Intel oneAPI DPC++/C++ Compiler Runtime versions antérieures à 2022.0
- Intel MPI Library pour Intel oneAPI HPC Toolkit versions antérieures à 2021.6
- Intel SGX SDK software pour Linux versions antérieures à 2.16.100.1
- Intel SGX SDK software pour Windows versions antérieures à 2.15.100.1
- Intel Quartus Prime Pro edition versions antérieures à 22.2
- Intel Quartus Prime Standard edition versions antérieures à 22.1STD
- Intel DSA versions antérieures à 22.4.26
- Intel Battery Life Diagnostic Tool versions antérieures à 2.2.0

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 Edition versions antérieures à 21.3
- Intel Quartus Prime Standard Edition versions antérieures à 21.1
- Intel FPGA SDK pour OpenCL Pro Edition versions antérieures à 22.1
- Intel SUR versions antérieures à 2.4.8902
- Intel Media SDK versions antérieures à 22.2.2
- Intel Open CAS versions antérieures à 22.3.1
- Micrologiciel Intel BMC versions antérieures à 2.86
- Micrologiciel Intel BMC versions antérieures à 2.09
- Micrologiciel Intel BMC versions antérieures à 2.78
- Intel OpenBMC versions antérieures à 0.72
- Intel OpenBMC versions antérieures à wht-1.01-61
- Intel OpenBMC versions antérieures à egs-0.91-179
- Intel FCS server versions antérieures à 1.1.79.3
- Intel Crypto API Toolkit pour Intel SGX versions antérieures à 2.0 ID commit 91ee496
- Les pilotes Intel Ethernet 500 Series Controller pour VMWare versions antérieures à 1.10.0.13
- Les pilotes Intel QAT pour Linux versions antérieures à 4.17
- Les pilotes Intel QAT pour Windows versions antérieures à 1.6
- Les pilotes Intel Ethernet Controller Administrative Tools pour Windows versions antérieures à 1.5.0.2
- Les pilotes Intel Iris Xe MAX pour Windows versions antérieures à 100.0.5.1474
- Intel 700 Series Ethernet Controllers and Adapters versions antérieures à 9.101
- Intel E810 Ethernet Controllers and Adapters versions antérieures à 1.7.0.8
- Intel SPS firmware versions antérieures à SPS_E5_04.04.04.300.0
- Intel SPS firmware versions antérieures à SPS_E3_06.00.03.300.0
- Intel CVAT versions antérieures à 2.0.1
- Intel Integrated Sensor Solution versions antérieures à 5.4.2.4579v3
- Intel Integrated Sensor Solution versions antérieures à 5.4.1.4479
- Intel Integrated Sensor Solution versions antérieures à 5.0.0.4143
- Intel EMA versions antérieures à 1.8.1.0
- Intel QATzip versions antérieures à 1.0.9
- Intel OFU versions antérieures à 14.1.28
- Les applications Android Intel ON Event Series versions antérieures à 2.0
- Intel Administrative Tools pour Intel Network Adapters versions antérieures à 27.3

- Intel Non-Volatile Memory (NVM) Update Utility pour Intel Ethernet Network Adapter E810 Series versions antérieures à 4.01
- Les processeurs Intel dont la liste est mentionnée dans les liens des fabriquants de la section Documentation.

Identificateurs externes

- CVE-2021-0187 , CVE-2021-33104 , CVE-2021-39295 , CVE-2021-39296 , CVE-2022-21163 , CVE-2022-21216 , CVE-2022-25905 , CVE-2022-25987 , CVE-2022-25992 , CVE-2022-26032 , CVE-2022-26052 , CVE-2022-26062 , CVE-2022-26076 , CVE-2022-26343 , CVE-2022-26345 , CVE-2022-26421 , CVE-2022-26425 , CVE-2022-26509 , CVE-2022-26512 , CVE-2022-26837 , CVE-2022-26840 , CVE-2022-26841 , CVE-2022-26843 , CVE-2022-26888 , CVE-2022-27170 , CVE-2022-27234 , CVE-2022-27808 , CVE-2022-29493 , CVE-2022-29494 , CVE-2022-29514 , CVE-2022-29523 , CVE-2022-30339 , CVE-2022-30530 , CVE-2022-30531 , CVE-2022-30539 , CVE-2022-30692 , CVE-2022-30704 , CVE-2022-31476 , CVE-2022-32231 , CVE-2022-32570 , CVE-2022-32575 , CVE-2022-32764 , CVE-2022-32971 , CVE-2022-33190 , CVE-2022-33196 , CVE-2022-33892 , CVE-2022-33902 , CVE-2022-33946 , CVE-2022-33964 , CVE-2022-33972 , CVE-2022-34153 , CVE-2022-34157 , CVE-2022-34346 , CVE-2022-34841 , CVE-2022-34843 , CVE-2022-34849 , CVE-2022-34854 , CVE-2022-34864 , CVE-2022-35729 , CVE-2022-35883 , CVE-2022-36278 , CVE-2022-36287 , CVE-2022-36289 , CVE-2022-36348 , CVE-2022-36369 , CVE-2022-36382 , CVE-2022-36397 , CVE-2022-36398 , CVE-2022-36416 , CVE-2022-36794 , CVE-2022-36797 , CVE-2022-37329 , CVE-2022-37340 , CVE-2022-38056 , CVE-2022-38090 , CVE-2022-41314 , CVE-2022-41614

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 Février 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 Février 2023 :

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