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	46071602/24
Date de Publication	15 Février 2024
Risque	Important
Impact	Important

Systèmes affectés

- ACAT software maintenu par Intel versions antérieures à 2.0.0
- Arm DS software pour Intel SoC FPGA versions antérieures à 2022.2
- Installation software pour Administrative Tools pour Intel Network Adapters versions antérieures à 28.2
- Installation software pour Intel Ethernet Adapter Complete Driver Pack versions antérieures à 28.2
- Installation software pour Intel Ethernet Connections Boot Utility, Preboot Images et pilotes EFI s versions antérieures à 28.2
- Intel Advisor pour oneAPI versions antérieures à 2023.2.0
- Intel Battery Life Diagnostic Tool software versions antérieures à 2.3.1
- Intel Binary Configuration Tool software versions antérieures à 3.4.4
- Intel CIP software versions antérieures à 2.4.10577
- Intel Chipset Driver Software versions antérieures à 10.1.19444.8378
- Intel Cluster Checker 2021.7.3
- Intel DSA software versions antérieures à 23.4.33
- Intel Distribution pour Python 2023.1
- Intel IPP Cryptography versions antérieures à 2021.8.0
- Intel ISPC versions antérieures à 1.21.0
- Intel Inspector pour oneAPI versions antérieures à 2023.2.0
- Intel Integrated Performance Primitives 2021.9.0
- Intel Killer Wi-Fi software version antérieures à 3.1423.712

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 MAS software versions antérieures à 2.3
- Intel MPI Library software versions antérieures à 2021.11
- Intel MPI Library versions antérieures à 2021.10.0
- Intel OFU software versions antérieures à 14.1.31
- Intel Optane PMem 100 Series management software versions antérieures à 01.00.00.3547
- Intel Optane PMem 200 Series management software versions antérieures à 02.00.00.3915
- Intel Optane PMem 300 Series management software versions antérieures à 03.00.00.0483
- Intel Optimization pour TensorFlow versions antérieures à 2.13.0
- Intel PCM software versions antérieures à 202307
- Intel PM software toutes versions
- Intel PROSet/Wireless Wi-Fi software versions antérieures à 22.240
- Intel QSFP+ Configuration Utility software toutes versions
- Intel SDK pour OpenCL Applications software toutes versions
- Intel SGX DCAP software pour Windows versions antérieures à 1.19.100.3
- Intel SPS versions antérieures à SPS_E5_06.01.04.002.0
- Intel SSU software versions antérieures à 3.0.0.2
- Intel SUR software versions antérieures à 2.4.10587
- Intel System Usage Report pour Gameplay Software version 2.0.1901
- Intel Trace Analyzer and Collector 2021.10.0
- Intel Unison software versions antérieures à C15
- Intel Unite Client software versions antérieures à 4.2.35041
- Intel VROC software versions antérieures à 8.0.8.1001
- Intel VTune Profiler pour oneAPI versions antérieures à 2023.2.0
- Intel XTU software versions antérieures à 7.12.0.29
- Intel oneAPI AI Analytics Toolkit 2023.2
- Intel oneAPI Base Toolkit versions antérieures à 2023.2.0
- Intel oneAPI Deep Neural Network Library versions antérieures à 2023.2.0
- Intel oneAPI HPC Toolkit versions antérieures à 2023.2.0
- Intel oneAPI IoT Toolkit versions antérieures à 2023.2.0.
- Intel oneAPI Math Kernel Library versions antérieures à 2023.2.0.
- Intel oneAPI Threading Building Blocks versions antérieures à 2021.10.0.

- Intel oneAPI Toolkit et du programme d'installation des composants versions antérieures à 4.3.2
- Micrologiciel du contrôleur Intel JHL8440 Thunderbolt 4 versions antérieures à 41
- Pilote Intel Thunderbolt DCH pour Windows versions antérieures à 88
- Pilotes Intel QAT software pour Windows versions antérieures à QAT1.7-W-1.11.0
- Sapphire Rapids Eagle Stream avec les processeurs Intel Xeon Scalable de 4e génération versions antérieures à PLR4 Release
- Tous les processeurs Intel Core de 6e, 7e, 8e ou 9e génération avec le pilote Intel Thunderbolt DCH toutes versions

Identificateurs externes

- CVE-2022-43701 CVE-2022-43702 CVE-2022-43703 CVE-2023-22293 CVE-2023-22311 CVE-2023-22342 CVE-2023-22390 CVE-2023-22848 CVE-2023-24463 CVE-2023-24481 CVE-2023-24542 CVE-2023-24589 CVE-2023-24591 CVE-2023-25073 CVE-2023-25174 CVE-2023-25769 CVE-2023-25777 CVE-2023-25779 CVE-2023-25945 CVE-2023-25951 CVE-2023-26585 CVE-2023-26586 CVE-2023-26591 CVE-2023-26592 CVE-2023-26596 CVE-2023-27300 CVE-2023-27301 CVE-2023-27303 CVE-2023-27307 CVE-2023-27308 CVE-2023-27517 CVE-2023-2804 CVE-2023-28374 CVE-2023-28396 CVE-2023-28407 CVE-2023-28715 CVE-2023-28720 CVE-2023-28739 CVE-2023-28745 CVE-2023-29153 CVE-2023-29162 CVE-2023-2976 CVE-2023-30767 CVE-2023-31189 CVE-2023-31271 CVE-2023-32280 CVE-2023-32618 CVE-2023-32642 CVE-2023-32644 CVE-2023-32646 CVE-2023-32647 CVE-2023-32651 CVE-2023-33870 CVE-2023-33875 CVE-2023-34315 CVE-2023-34351 CVE-2023-34983 CVE-2023-35003 CVE-2023-35060 CVE-2023-35061 CVE-2023-35062 CVE-2023-35121 CVE-2023-35769 CVE-2023-36490 CVE-2023-36493 CVE-2023-38135 CVE-2023-38561 CVE-2023-38566 CVE-2023-39425 CVE-2023-39432 CVE-2023-39932 CVE-2023-39941 CVE-2023-40154 CVE-2023-40156 CVE-2023-40161 CVE-2023-41090 CVE-2023-41091 CVE-2023-41231 CVE-2023-41252 CVE-2023-42776

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 13 Février 2024 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 13 Février 2024:

- 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