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	47491605/24
Date de Publication	16 Mai 2024
Risque	Important
Impact	Important

Systèmes affectés

- Programme de désinstallation Intel Driver & Support Assistant (DSA) versions antérieures à 23.4.39.10
- Processeurs Intel Core Ultra, plateforme Meteor Lake sans les derniers correctifs de sécurité
- Pilote Onboard vidéo versions antérieures à 1.14 pour Intel Server Boards basés sur des puces Intel 62X
- Pilote Intel Thunderbolt versions antérieures à 89
- Micrologiciels pour Intel Stratix 10 FPGA et SoC FPGA versions antérieures à 23.3
- Micrologiciels pour Intel Agilex 7 FPGA et SoC FPGA versions antérieures à 23.3
- Micrologiciel UEFI pour Intel Server M50FCP sans les derniers correctifs de sécurité
- Micrologiciel UEFI pour Intel Server D50DNP sans les derniers correctifs de sécurité
- Micrologiciel UEFI pour Intel Server Board S2600BP toutes versions
- Micrologiciel Intel Ethernet Controller I225 Manageability versions antérieures à NVM 1.87
- Micrologiciel Intel Bios PPAM sans les derniers correctifs de sécurité
- Micrologiciel Intel Bios Guard sans les derniers correctifs de sécurité
- Logiciels Intel PROSet/Wireless WiFi et Bluetooth versions antérieures à 23.20
- Intel oneVPL versions antérieures à 23.3.5
- Intel oneAPI HPC Toolkit versions antérieures à 2024.0.1.
- Intel oneAPI Base Toolkit versions antérieures à 2024.0
- Intel VTune Profiler versions antérieures à 2024.0

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 Trust Domain Extensions (TDX) module versions antérieures à TDX_1.5.05.46.698
- Intel Trace Analyzer and Collector versions antérieures à 2022.0.0 publiées en novembre 2023
- Intel Stratix 10 FPGA et SoC FPGA versions antérieures à 2.9.0
- Intel Quartus Prime Lite, Standard et Pro Design versions antérieures à 23.1
- Intel Processor Identification Utility-Legacy versions antérieures à 6.10.34.1129
- Intel Processor Identification Utility versions antérieures à 7.1.6
- Intel Processor Diagnostic Tool versions antérieures à 4.1.9.41
- Intel Power Gadget toutes versions
- Intel Performance Counter Monitor (PCM) versions antérieures à 202311
- Intel Neural Compressor versions antérieures à 2.5.0
- Intel Media SDK toutes versions
- Intel Inspector versions antérieures à 2024.0
- Intel HPC Toolkit versions antérieures à 2024.0
- Intel Graphics Performance Analyzers (GPA) versions antérieures à 2023.4.
- Intel Graphics Performance Analyzers (GPA) Framework versions antérieures à 2023.4.
- Intel Graphics Command Center Service embarqué dans le pilote Intel Graphics Windows DCH versions antérieures à 31.0.101.3790 et 31.0.101.2114
- Intel Extreme Tuning Utility (XTU) versions antérieures à 7.14.0.15
- Intel Ethernet Connections Boot Utility, Preboot Images et EFI Drivers versions antérieures à 28.3
- Intel Ethernet Adapters versions antérieures à 29.0.1
- Intel Ethernet Adapter Complete Driver Pack versions antérieures à 28.3
- Intel Dynamic Tuning Technology (DTT) sans les derniers correctifs de sécurité
- Intel Dynamic Load Balancer versions antérieures à 8.5.0
- Intel Distribution pour GDB versions antérieures à 2024.0
- Intel Data Center GPU Max Series 1100 and 1550 toutes versions
- Intel Context Sensing Technology (CST) versions antérieures à 2.1.10300
- Intel Computing Improvement Program versions antérieures à 2.4.10654
- Intel Code Base Investigator (CBI) versions antérieures à 1.1.0
- Intel Chipset Device Software versions antérieures à 10.1.19444.8378
- Intel Arc Control versions antérieures à 1.73.5335.2
- Intel Arc & Iris Xe Graphics versions antérieures à 31.0.101.5081

- Intel Agilex 7 FPGA et SoC FPGA versions antérieures à 2.9.0
- Intel Advisor versions antérieures à 2024.0
- Installateur Endurance Gaming Mode versions antérieures à 1.3.937.0
- Bibliothèque Libva versions antérieures à 2.20.0
- Bibliothèque Libva iotg-lin-gfx-libva toutes versions

Identificateurs externes

- CVE-2021-33141 CVE-2021-33142 CVE-2021-33145 CVE-2021-33146 CVE-2021-33157 CVE-2021-33158 CVE-2021-33161 CVE-2021-33162 CVE-2022-37341 CVE-2022-37410 CVE-2022-42879 CVE-2023-22656 CVE-2023-22662 CVE-2023-24460 CVE-2023-25952 CVE-2023-27305 CVE-2023-27504 CVE-2023-28383 CVE-2023-28402 CVE-2023-29165 CVE-2023-35192 CVE-2023-38417 CVE-2023-38420 CVE-2023-38581 CVE-2023-38654 CVE-2023-39433 CVE-2023-39929 CVE-2023-40070 CVE-2023-40071 CVE-2023-40155 CVE-2023-40536 CVE-2023-41082 CVE-2023-41092 CVE-2023-41234 CVE-2023-41961 CVE-2023-42433 CVE-2023-42668 CVE-2023-42773 CVE-2023-43487 CVE-2023-43629 CVE-2023-43745 CVE-2023-43748 CVE-2023-43751 CVE-2023-45217 CVE-2023-45221 CVE-2023-45315 CVE-2023-45320 CVE-2023-45733 CVE-2023-45736 CVE-2023-45743 CVE-2023-45745 CVE-2023-45845 CVE-2023-45846 CVE-2023-46103 CVE-2023-46689 CVE-2023-46691 CVE-2023-47165 CVE-2023-47169 CVE-2023-47210 CVE-2023-47282 CVE-2023-47855 CVE-2023-47859 CVE-2023-48368 CVE-2023-48727 CVE-2023-49614 CVE-2024-21772 CVE-2024-21774 CVE-2024-21777 CVE-2024-21788 CVE-2024-21792 CVE-2024-21809 CVE-2024-21813 CVE-2024-21814 CVE-2024-21818 CVE-2024-21823 CVE-2024-21828 CVE-2024-21831 CVE-2024-21835 CVE-2024-21837 CVE-2024-21841 CVE-2024-21843 CVE-2024-21861 CVE-2024-21862 CVE-2024-21864 CVE-2024-22015 CVE-2024-22095 CVE-2024-22379 CVE-2024-22382 CVE-2024-22384 CVE-2024-22390 CVE-2024-22476 CVE-2024-23487 CVE-2024-23980 CVE-2024-24971 CVE-2024-24981

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les versions susmentionnées de Intel. Un attaquant pourrait exploiter ces failles afin de porter atteinte à la confidentialité des données, de causer un déni de service, de réussir une élévation de privilèges et de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Intel du 15 Mai 2024 pour plus d'information.

Risque

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

Annexe

Bulletin de sécurité Intel du 15 Mai 2024:

- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00756.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00814.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00831.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00916.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00935.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00937.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00962.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00965.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00983.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00984.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00996.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01007.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01012.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01013.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01020.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01021.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01031.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01032.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01034.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01035.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01036.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01037.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01039.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: 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-01041.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01042.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01043.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01047.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01050.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01051.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01052.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01053.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01054.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01055.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01056.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01059.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01066.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01067.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01069.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01080.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01084.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01109.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