ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant des produits d'Intel
Numéro de Référence	39151011/22
Date de publication	10 Novembre 2022
Risque	Important
Impact	Important

Systèmes affectés

- Intel NUC BIOS Firmware sans la dernière mise à jour
- Intel NUC Kit Wireless Adapter driver installer software versions antérieures à 22.40.0
- Intel Support Android application versions antérieures à 22.02.28
- Intel WAPI Security sans la dernière mise à jour
- Intel EMA versions antérieures à 1.8.0
- Intel Advanced Link Analyzer Pro versions antérieures à 22.2
- Intel Advanced Link Analyzer Standrad versions antérieures à 22.1.1 STD
- Intel DCM versions antérieures à 5.0
- PresentMon versions antérieures à 1.7.1
- Intel SDP Tool versions antérieures à 3.0.0
- Intel Server System R1000WF, R200WF et Intel Server Board S2600WF sans la dernière mise à jour
- Intel Server Board M50CYP sans la dernière mise à jour
- Intel Server Board M10JNP sans la dernière mise à jour
- Intel PROSet/Wireless WiFi versions antérieures à 22.140
- Killer WiFi versions antérieures à 3.1122.3158
- Les produits Intel vPRO CSME WiFi sans la dernière mise à jour
- Intel PROSet/Wireless WiFi UEFI drivers versions antérieures à 2.2.14.22176
- Hyperscan library versions antérieures à 5.4.0
- Intel SGX SDK software pour Linux versions antérieures à 2.18.100.1
- Intel SGX SDK software pour Windows versions antérieures à 2.17.100.1
- Intel NUC HDMI Firmware Update Tool pour NUC7i3DN, NUC7i5DN et NUC7i7DN versions antérieures à 1.78.2.0.7.
- Intel Processors sans la dernière mise à jour

- Intel XMM 7560 Modem M.2 sans la dernière mise à jour
- Intel AMT SDK versions antérieures à 16.0.4.1
- Intel EMA versions antérieures à 1.7.1
- Intel MC versions antérieures à 2.3.2
- Intel VTune Profiler software versions antérieures à 2022.2.0
- Intel Glorp gaming particle physics demonstration software version 1.0.0
- Intel Quartus Prime Pro edition software versions antérieures à 22.1
- Intel Quartus Prime Standard edition software versions antérieures à 21.1 Patch 0.02std
- Intel Distribution of OpenVINO Toolkit versions antérieures à 2021.4.2
- Intel CSME versions antérieures à 11.8.93, 11.22.93, 11.12.93, 12.0.92, 14.1.67, 15.0.42, 16.1.25
- Intel AMT versions antérieures à 11.8.93, 11.22.93, 12.0.92, 14.1.67, 15.0.42, 16.0
- Intel SPS versions antérieures à SPS_E3_04.01.04.700.0, SPS_E3_06.00.03.035.0
- Intel System Studio toutes versions

Identificateurs externes

CVE-2022-26047	CVE-2021-33164	CVE-2022-33176	CVE-2022-37345
CVE-2022-21794	CVE-2022-34152	CVE-2022-36789	CVE-2022-35276
CVE-2022-38099	CVE-2022-26124	CVE-2022-36370	CVE-2022-37334
CVE-2022-36349	CVE-2022-36400	CVE-2022-36384	CVE-2022-36380
CVE-2022-36377	CVE-2022-30691	CVE-2022-36367	CVE-2022-33973
CVE-2022-30297	CVE-2022-27638	CVE-2022-33942	CVE-2022-26086
CVE-2022-26508	CVE-2022-30542	CVE-2021-0185	CVE-2022-29486
CVE-2022-27499	CVE-2022-26024	CVE-2022-26006	CVE-2022-21198
CVE-2022-28667	CVE-2022-26513	CVE-2022-27874	CVE-2022-28611
CVE-2022-26369	CVE-2022-28126	CVE-2022-26367	CVE-2022-26079
CVE-2022-27639	CVE-2022-26045	CVE-2022-26341	CVE-2022-26028
CVE-2022-30548	CVE-2022-27187	CVE-2022-27233	CVE-2022-26845
CVE-2022-27497	CVE-2022-29893	CVE-2021-33159	CVE-2022-29466
CVE-2022-29515	CVE-2021-33064		

Bilan de la vulnérabilité

Intel annonce la disponibilité de mises à jour de sécurité qui corrigent des vulnérabilités critiques affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d’accéder à des données confidentielles, d’élever ses privilèges ou de causer un déni de service.

Solution

Veuillez-vous référer aux bulletins de sécurité d'Intel pour appliquer les correctifs nécessaires

Risque

- Accès à des informations confidentielles.
- Elévation de privilèges.
- Déni de service.

Référence

Bulletins de sécurité d'Intel :

- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00752.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00747.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00740.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00720.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00716.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00715.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00713.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00711.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00710.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00708.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00699.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00695.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00691.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00689.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00688.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00687.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00683.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00680.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00676.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00673.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00659.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00642.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
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-00610.html
- https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00558.html