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	37731108/22
Date de Publication	11 Aout 2022
Risque	Important
Impact	Important

Systèmes affectés

- Intel Processors
- Intel NUCs versions antérieures à BC0076
- Intel AMT toutes versions
- Intel Standard Manageability toutes versions
- Intel Team Blue toutes versions
- Intel Datacenter Group Event Advisory iOS toutes versions
- Intel SEAPI toutes versions
- Open AMT Cloud Toolkit versions antérieures à 2.0.2 et 2.2.2
- Intel Distribution pour Python versions antérieures à 2022.0.3
- Intel DSA versions antérieures 22.2.14
- Intel Datacenter Group Event Android toutes versions
- Intel Enpirion Digital Power Configurator GUI toutes versions
- Intel SPS versions antérieures à SPS_E3_04.08.04.330.0 et SPS_E3_04.01.04.530.0
- Intel RST versions antérieures à 16.8.4.1011, 17.7.1.1010, 18.1.6.1039, 18.2.1.1008 et 18.3.0.1003
- Intel IPP Cryptography versions antérieures à 2021.5
- Intel NUC9 Extreme Laptop kits versions antérieures à 2.2.0.22
- Intel Data Center Manager versions antérieures à 4.1
- Intel Support Android versions antérieures à 21.7.40
- Intel VTune™ Profiler versions antérieures à 2022.2.0

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 HAXM versions antérieures à 7.7.1
- Intel Edge Insights pour les versions Industrial antérieures à 2.6.1
- Intel Ethernet 500 Series Controller drivers pour les versions VMware antérieures à 1.11.4.0
- Intel Ethernet 700 Series Controller drivers pour les versions VMware antérieures à 2.1.5.0
- Intel Wireless Bluetooth versions antérieures à 22.120
- Intel Killer™ Bluetooth versions antérieures à 22.120
- Intel PROSet/Wireless WiFi versions antérieure à 22.120
- Intel Killer™ WiFi versions antérieures à 3.1122.1105
- Intel Connect M Android versions antérieures à 1.7.4
- Intel 700 Series Ethernet contrôleurs et adaptateurs versions antérieures à 8.5
- Intel 722 Series Ethernet contrôleurs et adaptateurs versions antérieures à 1.5.5
- Intel E810 Ethernet contrôleurs et adaptateurs versions antérieures à 1.6.1.9

Identificateurs externes

- CVE-2022-28858 CVE-2022-33209 CVE-2022-27493 CVE-2022-34488 CVE-2022-32579 CVE-2022-34345 CVE-2022-30601 CVE-2022-30944 CVE-2022-28697 CVE-2022-26373 CVE-2022-29507 CVE-2022-30296 CVE-2022-26844 CVE-2022-26344 CVE-2022-26374 CVE-2022-25899 CVE-2021-33060 CVE-2022-28696 CVE-2022-26017 CVE-2022-25841 CVE-2022-25999 CVE-2022-26074 CVE-2018-1285 CVE-2022-26083 CVE-2022-21229 CVE-2022-21225 CVE-2022-23182 CVE-2022-24378 CVE-2022-23403 CVE-2022-27500 CVE-2022-21807 CVE-2022-21233 CVE-2022-21812 CVE-2022-22730 CVE-2022-25966 CVE-2022-21148 CVE-2022-21152 CVE-2022-21793 CVE-2021-33847 CVE-2021-26257 CVE-2021-26950 CVE-2021-23179 CVE-2022-21181 CVE-2021-37409 CVE-2021-23223 CVE-2021-23168 CVE-2021-44545 CVE-2021-26254 CVE-2022-21172 CVE-2022-21240 CVE-2022-21139 CVE-2022-21197 CVE-2022-21160 CVE-2021-23188 CVE-2022-21212 CVE-2022-21140 CVE-2021-44470 CVE-2021-33126 CVE-2021-33128 CVE-2022-28709

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 provoquer un déni de service à distance et de réussir une élévation de privilèges.

Solution

Veuillez se référer au bulletin de sécurité Intel du 09 Aout 2022 pour plus d'information.

Risque

- Déni de service,
- Atteinte à la confidentialité des données,

- Elévation de privilèges

Annexe

Bulletin de sécurité Intel du 09 Aout 2022 :

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