



BULLETIN DE SECURITE

Titre : Vulnérabilités dans plusieurs produits Intel

Numéro de Référence : 20811406/19

Risque : Important

Impact : Important

Systemes affectés

- Intel RAID Web Console 3 pour Windows versions antérieures à 7.009.011.000
- Intel Omni-Path Fabric Manager GUI versions antérieures à 10.9.2.1.1
- Intel Core X-series Processors, 4th Generation Intel Core i5 Processors, 4th Generation Intel Core i3 Processors, Intel Pentium Processor G Series, Intel Pentium Processor 3000 Series, Intel Celeron Processor 2000 Series, Intel Xeon Processor E7 v3 Family, Intel Xeon Processor E5 v3 Family et Intel Xeon Processor E3 v3 Family
- Intel Turbo Boost Max Technology 3.0 microiciels versions 1.0.0.1035 et antérieures
- Intel SGX Linux client driver versions antérieures à 2.5
- Intel SGX DCAP Linux driver versions antérieures à 1.1
- Intel PROSet/Wireless WiFi Software versions antérieures à 21.10 pour Microsoft Windows 7, 8.1 et 10
- Intel Accelerated Storage Manager dans Intel RSTe versions antérieures à 5.5.0.2015
- Intel Chipset Device Software (INF Update Utility) versions antérieures à 10.1.1.45
- ITE Tech Consumer Infrared Driver pour Windows 10 versions antérieures à 5.4.3.0
- Intel NUC

Identificateurs externes

- CVE-2019-11123 CVE-2019-11124 CVE-2019-11125 CVE-2019-11126 CVE-2019-11127
- CVE-2019-11128 CVE-2019-11129 CVE-2019-11119 CVE-2019-11117 CVE-2019-0179
- CVE-2019-0180 CVE-2019-0178 CVE-2019-0177 CVE-2019-0175 CVE-2019-0181
- CVE-2019-0182 CVE-2019-0183 CVE-2019-11092 CVE-2019-0174 CVE-2019-0164
- CVE-2019-0157 CVE-2019-0136 CVE-2019-0130 CVE-2019-0128 CVE-2018-3702

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans certains produits Intel. Un attaquant pourrait exploiter ces failles afin de provoquer un déni de service à distance, de réussir une élévation de privilèges et de porter atteinte à l'intégrité des données.

Solution :

Veillez-vous référer aux bulletins de sécurité Intel du 11 Juin 2019 afin d'installer les nouvelles mises à jour:

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00264.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00259.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00257.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00248.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00247.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00243.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00235.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00232.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00226.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00224.html>

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00206.html>

Risque :

- Déni de service à distance,
- Porter Atteinte à l'intégrité des données,
- Élévation de privilèges.

Référence :

- Bulletin de sécurité Intel du 11 Juin 2019 :
<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00264.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00259.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00257.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00248.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00247.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00243.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00235.html>

- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00232.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00226.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00224.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00206.html>