



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits d'Intel
Numéro de Référence	50841411/24
Date de publication	14 Novembre 2024
Risque	Important
Impact	Important

Systèmes affectés

- Thunderbolt Share versions antérieures à la version 1.0.49.9
- Processeurs Intel Xeon W2400 et W3400 Fishhawk Falls Workstation CPU ID 806F8
- Processeurs Intel Xeon D Idaville Server CPU ID 606C1
- Processeurs Intel Xeon CPU Max Series Eagle Stream Server CPU ID 806F8
- Processeurs Intel Xeon 6 Sierra Forest Server CPUID A06F2
- Processeurs 5e génération Intel Xeon Scalable Eagle Stream Server CPUID C0F62
- Processeurs 4e génération Intel Xeon Silver Eagle Stream Server CPU ID 0x806f8
- Processeurs 4e génération Intel Xeon Scalable Eagle Stream Server CPU ID 0x806f8
- Processeurs 4e génération Intel Xeon Scalable avec Intel vRAN Eagle Stream Network et Edge CPU ID 806F8
- Processeurs 4e génération Intel Xeon Platinum Eagle Stream Server CPU ID 0x806f8
- Processeurs 4e génération Intel Xeon Gold Eagle Stream Server CPU ID 0x806f8
- Processeurs 4e génération Intel Xeon Edge Enhanced Eagle Stream Network et Edge CPU ID 806F8
- Processeurs 4e Generation Intel Xeon Bronze Eagle Stream Server CPU ID 0x806f8
- Processeurs 3e génération Intel Xeon Scalable Whitley Server Workstation CPU ID 606A6
- Pilotes Intel Data Center GPU Flex Series versions antérieures à la version 31.0.101.5522 pour Windows
- Pilotes Intel Arc et Iris Xe Graphics versions antérieures à la version 31.0.101.5518 pour Windows
- Pilote Intel Graphics 15.45 toutes les versions pour Windows
- Pilote Intel Graphics 15.40 6e Gen toutes les versions pour Windows 7 et 8.1
- Pilote Intel Graphics 15.40 4e Gen toutes les versions pour Windows 10
- Pilote Intel Arc Pro Graphics versions antérieures à la version 31.0.101.5525 pour Windows

- Pilote Intel Arc et Iris Xe Graphics versions antérieures à la version 30.0.101.5379 pour Windows
- Pilote Intel 7e à 10e Gen Processor Graphics versions antérieures à la version 31.0.101.2128 pour Windows
- OpenVINO Model Server versions antérieures à la version 2024.0
- Moteur Intel QAT pour OpenSSL versions antérieures à la version v1.6.1
- JAM STAPL Player versions antérieures à la version 2.6.1
- Intel Wireless-AC 9260 (ThP2) et Intel Killer Wi-Fi AX1550x/w2
- Intel Wi-Fi 6E AX211 (GfP2) et Intel Killer Wi-Fi AX1675i/s2
- Intel Wi-Fi 6E AX210 (TyP2) et Intel Killer Wi-Fi AX1675x/w2
- Intel Wi-Fi 6 AX200 (CcP2) et Intel Killer Wi-Fi AX1650x/w2
- Intel VTune Profiler versions antérieures à la version 2024.2.0
- Intel VROC versions antérieures à la version 8.6.0.3001
- Intel VPL versions antérieures à la version 24.1.4
- Intel SGX SDK pour Linux versions antérieures à la version 2.24
- Intel Server Board S2600ST toutes les versions
- Intel Server Board S2600BPBR toutes les versions
- Intel Server Board S2600BP toutes les versions
- Intel Server Board M70KLP toutes les versions
- Intel Server Board M20NTP toutes les versions
- Intel Server Board M10JNP2SB toutes les versions
- Intel Series management versions antérieures à la version CR_MGMT_02.00.00.4040 et CR_MGMT_03.00.00.0499 pour Optane PMem
- Intel SDP Tool toutes les versions pour Windows
- Intel Rendering Toolkit versions antérieures à la version 2024.1.0
- Intel Quartus Prime Standard Edition versions antérieures à la version 23.1.1 pour Windows
- Intel Quartus Prime Pro Edition versions antérieures à la version 24.2
- Intel PROSet/Wireless Intel Killer Wi-Fi et Intel Wireless Bluetooth versions 23.40
- Intel oneMKL versions antérieures à la version 2024.2 pour Windows
- Intel oneAPI HPC Toolkit versions antérieures à la version 2024.2
- Intel oneAPI Base Toolkit versions antérieures à la version 2024.2
- Intel Neural Compressor versions antérieures v3.0
- Intel Media Driver pour VAAPI versions antérieures à la version 24.1.1
- Intel MAS versions antérieures à la version 2.5
- Intel IPP versions antérieures à la version 2021.12.0
- Intel High Level Synthesis Compiler pour Intel Quartus Prime Pro Edition versions antérieures à la version 24.1
- Intel Graphics Offline Compiler pour OpenCL Code versions antérieures à la version 2024.1.0.142, pilotes graphiques 31.0.101.5445.
- Intel Granulate versions antérieures à la version 4.30.1
- Intel Fortran Compiler versions antérieures à la version 2024.2
- Intel Fortran Compiler Classic versions antérieures à la version 2021.13
- Intel Extension pour Transformers versions antérieures à la version 1.5
- Intel EMA versions antérieures à la version 1.13.1.0
- Intel DSA versions antérieures à la version 24.3.26.8

- Intel Distribution pour Python versions antérieures à la version 2024.2
- Intel CST versions antérieures à la version 8.7.10803
- Intel CIP versions antérieures à la version 2.4.10852
- Intel Binary Configuration Tool versions antérieures à la version 3.4.5
- Intel Advanced Link Analyzer Standard Edition installer versions antérieures à la version 23.1.1
- BigDL versions antérieures à la version 2.5.0
- ACAT versions antérieures à la version 3.11.0

Identificateurs externes

CVE-2022-34301	CVE-2024-21783	CVE-2024-21808	CVE-2024-21820	CVE-2024-21853
CVE-2024-23198	CVE-2024-23312	CVE-2024-23918	CVE-2024-23919	CVE-2024-24984
CVE-2024-25563	CVE-2024-25565	CVE-2024-25647	CVE-2024-28030	CVE-2024-28049
CVE-2024-28051	CVE-2024-28169	CVE-2024-28881	CVE-2024-28950	CVE-2024-28952
CVE-2024-29076	CVE-2024-29083	CVE-2024-29085	CVE-2024-31154	CVE-2024-31158
CVE-2024-31407	CVE-2024-32044	CVE-2024-32048	CVE-2024-32483	CVE-2024-32667
CVE-2024-33611	CVE-2024-33624	CVE-2024-34022	CVE-2024-34023	CVE-2024-34028
CVE-2024-34164	CVE-2024-34165	CVE-2024-34167	CVE-2024-34170	CVE-2024-34776
CVE-2024-35201	CVE-2024-35245	CVE-2024-36242	CVE-2024-36245	CVE-2024-36253
CVE-2024-36275	CVE-2024-36276	CVE-2024-36282	CVE-2024-36294	CVE-2024-36482
CVE-2024-36488	CVE-2024-37025	CVE-2024-37027	CVE-2024-38383	CVE-2024-38387
CVE-2024-38660	CVE-2024-38665	CVE-2024-38668	CVE-2024-39285	CVE-2024-39609
CVE-2024-39811	CVE-2024-40885	CVE-2024-41167		

Bilan de la vulnérabilité

Intel annonce la disponibilité de mises à jour de sécurité qui corrigent des vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire, d'élever ses privilèges de contourner des mesures de sécurité ou de causer un déni de service.

Solution

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

Risque

- Elévation de privilèges.
- Dénier de service.
- Exécution de code arbitraire
- Contournement de mesures de sécurité

Référence

Bulletins de sécurité d'Intel :

- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01219.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01217.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01204.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01201.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01200.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01197.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01196.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01195.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01193.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01191.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01190.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01189.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01188.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01187.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01183.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01182.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01179.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01177.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01176.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01175.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01173.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01167.html>

- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01165.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01163.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01161.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01158.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01155.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01154.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01151.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01148.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01146.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01145.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01142.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01140.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01138.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01132.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01131.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01111.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01108.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01101.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01085.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01079.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01076.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01024.html>