



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

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits d'Intel
Numéro de Référence	61021102/26
Date de publication	11 Février 2025
Risque	Important
Impact	Important

Systèmes affectés

- AI Playground software antérieures à la version 2.6.1 beta.
- Intel® MAS software antérieures à la version 2.5.2
- System Firmware Update Utility (SysFwUpdt) for Intel® Server Boards and Intel® Server Systems Based antérieures à la version 16.0.12.
- Intel® Server Chipset Driver Software antérieures à la version 10.1.20266.8668 for Windows for Intel® Server Boards and Systems Based on Intel® 741 Chipset.
- ESXi base driver (icen) for Intel® 800 Series Ethernet antérieures à la version 2.2.2.0 (ESXi 8.0).
- ESXi base driver (icen) for Intel® 800 Series Ethernet antérieures à la version 2.2.3.0 (ESXi 9.0).
- Intel® Atom P5000 family Snow Ridge NS
- Intel® Atom C5000 family Parker Ridge
- Intel® Atom P6000 family Grand Ridge BTS HCC
- Intel® Xeon® 6700P-B/6500P-B series SoC with P-Cores Granite Rapids-D
- Intel® Xeon® 6 with E-cores Sierra Forest SP
- Intel® NPU Driver for Linux versions antérieures à 1.24.0
- Intel® NPU Driver for Windows versions antérieures à 32.0.100.4297
- Intel® Xeon® 6 with E-cores Birch Stream
- Intel® Xeon® 6 with P-cores Birch Stream
- Intel® Battery Life Diagnostic Tool software antérieures à la version 2.7.
- 4th Gen Intel® Xeon® Scalable processor 1.5.20 et versions antérieures
- 5th Gen Intel® Xeon® Scalable processor 1.5.20 et versions antérieures
- Intel® Xeon® 6 processor with P-cores 2.0.12 et versions antérieures
- Intel® Xeon® 6 SoC 2.0.12 et versions antérieures

- Intel® Xeon® 6 processor with E-cores 1.5.20 et versions antérieures
- 10th Generation Intel® Core™ processor family
- 11th Generation Intel® Core processor family
- 11th Generation Intel® Core processor family
- Intel® Celeron® 6305RE, Intel® Celeron® 6305E, Intel® Core™ i3-1115GRE Intel® Core™ i3-1115G4E, Intel® Core™ i5-1145GRE, Intel® Core™ i5-1145G7E Intel® Core™ i7-1185GRE, Intel® Core™ i7-1185G7E
- 11th Generation Intel® Core processor family
- 11th Generation Intel® Core processor family
- 11th Generation Intel® Core processor family
- 11th Generation Intel® Core processor family
- Intel® Celeron® 6600HLE, Intel® Celeron® 6600HE, Intel® Core™ i3-11100HE
- Intel® Core™ i5-11500HE, Intel® Core™ i7-11850HE, Intel® Xeon® W-11155MLE
- Intel® Xeon® W-11555MLE, Intel® Xeon® W-11865MLE, Intel® Xeon® W-11865MRE
- Intel® Xeon® W-11555MRE, Intel® Xeon® W-11155MRE
- 11th Generation Intel® Core™ processor family
- Intel® Xeon® E-2300 processor family Intel® Xeon® W-1300 processor family
- 12th Generation Intel® Core™ processor family Intel® Pentium® Gold processor family Intel® Celeron® processor family
- 12th Generation Intel® Core™ processor family Intel® Pentium® Gold processor family Intel® Celeron® processor family
- 12th Generation Intel® Core™ processor family Intel® Pentium® Gold processor family Intel® Celeron® processor family
- 12th Generation Intel® Core™ processor family Intel® Pentium® Gold processor family Intel® Celeron® processor family
- 13th Generation Intel® Core™ Processor Family 14th Generation Intel® Core™ processor family Intel® Pentium® Gold processor family Intel® Celeron® processor family 13th Generation Intel® Core™ i7 processors
- Intel Pentium Processor
- G7400/G7400T Intel® Xeon® E processor family
- Intel® Core™ Ultra processors (Series 1)
- Intel® Core™ Ultra processors (Series 1)
- Intel® Core™ Ultra processors (Series 1)
- Intel® Core™ Ultra processors (Series 2)
- Intel® Core™ Ultra processors (Series 2)
- Intel® Core™ Ultra processors (Series 2)
- Intel® Core™ Ultra processors (Series 2)
- Intel® Core™ Ultra processors (Series 2)
- 3rd Generation Intel® Xeon® Scalable processor family
- Intel® Xeon® D processor family
- 4th Generation Intel® Xeon® Scalable processors 4th Generation Intel® Xeon® Platinum processors 4th Generation Intel® Xeon® Gold processors 4th Generation Intel® Xeon® Silver processor 4th Generation Intel® Xeon® Bronze processor Intel® Xeon® CPU Max Series processors 5th Generation Intel® Xeon® Scalable processors
- 4th Generation Intel® Xeon® Scalable processors 4th Generation Intel® Xeon® Platinum

processors 4th Generation Intel® Xeon® Gold processors 4th Generation Intel® Xeon® Silver processor 4th Generation Intel® Xeon® Bronze processor Intel® Xeon® CPU Max Series processors

- 4th Generation Intel® Xeon® Scalable processors 4th Generation Intel® Xeon® Platinum processors 4th Generation Intel® Xeon® Gold processors 4th Generation Intel® Xeon® Silver processor 4th Generation Intel® Xeon® Bronze processor Intel® Xeon® CPU Max Series processors
- Intel® Xeon® W Processors
- 5th Generation Intel® Xeon® Scalable processors
- Intel® Xeon® 6 processor with P-Cores
- Intel® Xeon® 6700P-B/6500P-B Series SoC with P-Cores
- Intel® Arc™ graphics versions antérieures à 32.0.101.7026
- Intel® Arc™ Pro graphics versions antérieures à 32.0.101.6979
- Intel® Iris® Xe graphics versions antérieures à 32.0.101.7026
- 7th-10th Gen Intel® Core™ processor family versions antérieures à 31.0.101.2137
- Intel Atom®, Pentium®, and Celeron® processors versions antérieures à 31.0.101.2137
- Intel® Server Firmware Update Utility software antérieures à la version 16.0.12.
- Intel® Server Board M50CYP Family BIOS and System Firmware Update Package (SFUP) for Windows and Linux antérieures à la version R01.01.0010.
- Intel® Server Board D50TNP Family BIOS and System Firmware Update Package (SFUP) for Windows and Linux antérieures à la version R01.01.0010.
- BIOS and System Firmware Update Package (SFUP) for Windows and Linux for Intel® Server D50DNP Family antérieures à la version R01.02.0004.
- BIOS and System Firmware Update Package (SFUP) for Windows and Linux for Intel® Server M50FCP Family antérieures à la version R01.02.0004.
- Intel® Optane™ PMem management software antérieures aux versions CR_MGMT_01.00.00.3584, CR_MGMT_02.00.00.4052, CR_MGMT_03.00.00.0538.
- Intel® C420 Chipset versions antérieures à 11.13.1
- Intel® X299 Chipset versions antérieures à 11.13.1
- Intel® C230 Series Chipset versions antérieures à 11.13.1
- 8th Gen Intel® Core™ processor versions antérieures à 11.9.5
- Intel® 200 Series Chipset versions antérieures à 11.9.5
- Intel® 100 Series Chipset versions antérieures à 11.9.5
- 8th Gen Intel® Core™ processor versions antérieures à 12.1.1
- 9th Gen Intel® Core™ processor versions antérieures à 12.1.1
- Intel® 300 Series Chipset versions antérieures à 12.1.1
- Intel® C240 Series Chipset versions antérieures à 12.1.1
- Pentium® Gold processor series (G54XXU) versions antérieures à 12.1.1
- Celeron® processor 4000 series versions antérieures à 12.1.1
- Intel® 400 Series Chipset versions antérieures à 14.1.79
- Intel® 500 Series Chipset versions antérieures à 15.0.55
- Intel® C250 Series Chipset versions antérieures à 15.0.55
- Intel® C740 Series Chipset versions antérieures à 15.20.25
- Intel® 600 Series Chipset versions antérieures à 16.1.40
- Intel® 700 series chipset versions antérieures à 16.1.40

- 5th Gen Intel® Xeon® Processor versions antérieures à 16.11.25
- Intel® Core™ Ultra Processors (Series 1) versions antérieures à 18.0.18
- Intel® Core™ Ultra Processors (Series 2) versions antérieures à 19.0.5
- Intel® Core™ Ultra Processors (Series 2) versions antérieures à 20.0.5
- 4th Gen Intel® Xeon® Scalable processor 1.5.16 et versions antérieures
- 5th Gen Intel® Xeon® Scalable processor 1.5.16 et versions antérieures
- Intel® Xeon® 6 processor with E-cores 1.5.24 et versions antérieures
- Intel® Xeon® 6 processor with P-cores 2.0.09 et versions antérieures
- Intel® Xeon® 6 processor SOC 2.0.09 et versions antérieures
- VTune™ Profiler software antérieures à la version 2025.0.
- Intel® oneAPI Base Toolkits antérieures à la version 2025.0.
- Intel® Ethernet Adapters 800 Series Controllers and associated adapters antérieures aux versions 30.3 ou qui viennent après.

Identificateurs externes

CVE-2025-20070	CVE-2025-20080	CVE-2025-20106	CVE-2025-22453	CVE-2025-22849
CVE-2025-22885	CVE-2025-24851	CVE-2025-25058	CVE-2025-25210	CVE-2025-27243
CVE-2025-27535	CVE-2025-27560	CVE-2025-27572	CVE-2025-27708	CVE-2025-27940
CVE-2025-30508	CVE-2025-30513	CVE-2025-31648	CVE-2025-31655	CVE-2025-31944
CVE-2025-32003	CVE-2025-32007	CVE-2025-32008	CVE-2025-32092	CVE-2025-32452
CVE-2025-32453	CVE-2025-32467	CVE-2025-32735	CVE-2025-32739	CVE-2025-33030
CVE-2025-35992	CVE-2025-35998	CVE-2025-35999	CVE-2025-36511	CVE-2025-36522

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'élever ses privilèges, d'accéder à des informations confidentielles ou de causer un déni de service.

Solution

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

Risque

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

Référence

Bulletins de sécurité d'Intel du 11 Novembre 2025 :

- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01415.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01414.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01412.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01411.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01408.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01406.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01403.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01401.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01399.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01397.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01396.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01385.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01325.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01323.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01315.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01314.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01265.html>
- <https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01171.html>