



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits d'Intel
Numéro de Référence	58371211/25
Date de publication	12 Novembre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Intel PRI Driver Software unquoted search path
- Intel MPI Library uncontrolled search path
- Intel Slim Bootloader UEFI Firmware protection mechanism
- Intel QuickAssist Technology improper authentication
- Intel QAT Windows Software buffer overflow
- Intel QuickAssist Technology Software untrusted pointer dereference
- Intel Arc B-series GPU Device Driver default permission
- Intel System Event Log Viewer Utility Software uncontrolled search path
- Intel ACAT toctou
- Intel QAT Windows Software out-of-bounds write
- Intel Neural Compressor Software neutralization
- Intel QAT Windows Software unusual condition
- Intel oneAPI DPC++C++ Compiler Software uncontrolled search path
- Intel Processor Identification Utility uncontrolled search path
- Intel Thread Director Visualizer software default permission
- Intel QAT Windows Software out-of-bounds
- Intel Graphics Software uncontrolled search path
- Intel PresentMon default permission
- Intel One Boot Flash Update Software default permission
- Intel Instrumentation and Tracing Technology API Software uncontrolled search path
- Intel QuickAssist Technology Software input validation
- Intel QAT Windows Software null pointer dereference
- Intel NPU Drivers protection mechanism
- Intel One Boot Flash Update Software uncontrolled search path

- Intel oneAPI Math Kernel Library denial of service
- Intel Driver and Support Assistant uncontrolled search path
- Intel UEFI Reference Platforms debug code
- Intel QAT Windows Software untrusted pointer dereference
- Intel Gaudi Software resource consumption
- Intel Processor Identification Utility default permission
- Intel NPU Driver dynamically-managed code resources
- Intel Graphics Drivers and Intel LTS kernels Device Driver denial of service
- Intel PROSet/Wireless WiFi Device Driver out-of-bounds write
- Intel PROSet/Wireless WiFi Device Driver out-of-bounds
- Intel Server Configuration Utility Software link following
- Intel PROSet/Wireless WiFi Device Driver insufficient control flow management
- Intel PresentMon access control
- Intel Ethernet Adapter Complete Driver Pack Software toctou
- Intel CIP Software unrestricted upload
- Intel CIP Software privileges management
- Intel Distribution for Python Software Installers uncontrolled search path
- Intel CIP Software protection mechanism
- Intel System Support Utility uncontrolled search path
- Intel CIP Software information disclosure
- Intel CIP Software access control
- Intel PROSet/Wireless WiFi denial of service
- Intel Killer Performance Suite software uncontrolled search path
- Intel CIP Software file inclusion
- Intel Display Virtualization Device Driver uncontrolled search path
- Intel VTune Profiler improper authentication
- Intel Processor Identification Utility unmaintained third party components
- Intel Rapid Storage Technology Application insecure inherited permissions
- Intel CIP Software uncontrolled search path
- Intel NPU Driver sensitive information in resource not removed before reuse
- Intel CIP Software input validation

Identificateurs externes

CVE-2025-32449	CVE-2025-35972	CVE-2025-35968	CVE-2025-33000	CVE-2025-32732
CVE-2025-32446	CVE-2025-32091	CVE-2025-31645	CVE-2025-27725	CVE-2025-27713
CVE-2025-27712	CVE-2025-32088	CVE-2025-32038	CVE-2025-32001	CVE-2025-31940
CVE-2025-31937	CVE-2025-31647	CVE-2025-30518	CVE-2025-27711	CVE-2025-31931
CVE-2025-30509	CVE-2025-26694	CVE-2025-26402	CVE-2025-25059	CVE-2025-31948
CVE-2025-30506	CVE-2025-30185	CVE-2025-27710	CVE-2025-27249	CVE-2025-27246
CVE-2025-26405	CVE-2025-25216	CVE-2025-35971	CVE-2025-35967	CVE-2025-24918
CVE-2025-35963	CVE-2025-33029	CVE-2025-32037	CVE-2025-31146	CVE-2025-30255
CVE-2025-24862	CVE-2025-24863	CVE-2025-30182	CVE-2025-24848	CVE-2025-24519
CVE-2025-24842	CVE-2025-24838	CVE-2025-24847	CVE-2025-24834	CVE-2025-24516
CVE-2025-24512	CVE-2025-24491	CVE-2025-20614	CVE-2025-20065	CVE-2025-20056

CVE-2025-20010 CVE-2025-24327 CVE-2025-20050 CVE-2025-20622 CVE-2025-24299
CVE-2025-24307 CVE-2025-24314

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 ou de causer un déni de service.

Solution

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

Risque

- Elévation de privilèges.
- Déni de service.

Référence

Bulletins de sécurité d'Intel du 11 Novembre 2025 :

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