AYI NEDJIMI Consultants

DMA FireWire & Thunderbolt 2026 : Inception, PCILeech

16 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 3780 mots • 16 vues •

> À retenir — Attaques DMA FireWire et Thunderbolt Les attaques DMA via FireWire et Thunderbolt permettent à un attaquant avec accès physique 5 min de bypass mot de passe.

À RETENIR

À retenir — Attaques DMA FireWire et Thunderbolt

Les attaques DMA via FireWire et Thunderbolt permettent à un attaquant avec accès physique 5 min de bypass mot de passe Windows/Linux, dumper RAM et ex credentials.

Outils 2026 : **Inception** (Carsten Maartmann-Moe), **PCILeech** (Ulf Frisk), **MemProcFS**, **LiME**, dispositifs FPGA Screamer M.2.

Pré-requis : interface DMA exposée (FireWire IEEE 1394, Thunderbolt 3/4, PCIe externe), IOMMU désactivée ou bypass, OS pré-2019 ou Kernel DMA Protection désactivée.

Défense critique : **Kernel DMA Protection** (Windows 10 1803+/11), VT-d/IOMMU activé BIOS, BitLocker + TPM-only avec pré-boot PIN, désactivation Thunderbolt PCIe si non utilisée.

Surface attaque réelle 2026 : laptops entreprise non patchés, salles serveurs (FireWire/eSATA legacy), KVM-over-IP en datacenter, kiosques publics.

Les **attaques DMA** (Direct Memory Access) via **FireWire** (IEEE 1394) et **Thunderbolt** exploitent une primitive simple : tout périphérique branché en DMA peut lire et écrire la RAM système sans passer par le CPU ni l'OS. Avec accès physique 5 minutes et un câble FireWire ou Thunderbolt, un attaquant dumpe la mémoire d'un laptop verrouillé, patche le bypass du mot de passe Windows ou Linux, extrait clés BitLocker, tokens Kerberos, hashes LSASS. Documentée publiquement depuis 2004 (Maximillian Dornseif), industrialisée avec Inception (2011) puis PCILeech (2016), la classe d'attaques reste pertinente en 2026 — Apple Silicon, Windows 11 24H2 et nombreux laptops Linux la mitigent partiellement seulement. Cet article documente les vecteurs FireWire et Thunderbolt act
2026, et les défenses concrètes pour postes entrepri

Réponse sous 24h

Devis gratuit →