NVD DB Update

CVE-2025-1945 - Score: 9.8

Components:

mmaitre314 picklescan *

Description:

picklescan before 0.0.23 fails to detect malicious pickle files inside PyTorch model archives when certain ZIP file flag bits are modified. By flipping specific bits in the ZIP file headers, an attacker can embed malicious pickle files that remain undetected by PickleScan while still being successfully loaded by PyTorch's torch.load(). This can lead to arbitrary code execution when loading a compromised model.

Main problems:

345 no CWE Description available

https://cybersword.tech
www.linkedin.com/in/cybersword-tech
ph1sher
@davidwowa