Performance Comparison: Vanilla vs Adversarial Training

Clean Accuracy

- Vanilla EfficientNet-B0: 59.09%
- Adversarial Training: 49.27%

Robust Accuracy (FGSM ε=8/255)

- Vanilla EfficientNet-B0: 4.73%
- Adversarial Training: 34.55%

Training Time (3 epochs, CPU)

- Vanilla EfficientNet-B0: 0.063h
- Adversarial Training: 0.121h