Commit 03c8082

ColeMurray and **vasqu** authored on Jan 12 · ✕ 18 / 26 · Verified

```
Fix unsafe torch.load() in _load_rng_state allowing arbitrary code execution
(#43140)

* Fix unsafe torch.load() in _load_rng_state allowing arbitrary code execution

Add weights_only=True to torch.load() call in Trainer._load_rng_state()
to prevent arbitrary code execution when loading malicious checkpoint files.

The existing safe_globals() context manager provides no protection for
PyTorch < 2.6 as it returns contextlib.nullcontext(). This makes the
torch.load() call at line 3059 vulnerable to pickle deserialization
attacks, unlike all other torch.load() calls in the same file which
correctly use weights_only=True.

Impact: Users loading untrusted checkpoints on PyTorch 2.2-2.5 are
vulnerable to arbitrary code execution via malicious rng_state.pth files.

* Update src/transformers/trainer.py

Co-authored-by: Anton Vlasjuk <73884904+vasqu@users.noreply.github.com>

---------

Co-authored-by: Anton Vlasjuk <73884904+vasqu@users.noreply.github.com>
```

main (#43140) · v5.5.0 ••• v5.0.0rc3

1 parent 2aa7b65 commit 03c8082

1 file changed +2 -1 lines changed

Top

Filter files...

src/transformers

trainer.py

1 file changed +2 -1 lines changed

Search within code

src/transformers/trainer.py

```
@@ -3056,7 +3056,8 @@ def _load_rng_state(self, checkpoint):
3056  3056                  return
3057  3057
3058  3058          with safe_globals():
3059        -             checkpoint_rng_state = torch.load(rng_file)
      3059  +             check_torch_load_is_safe()
      3060  +             checkpoint_rng_state = torch.load(rng_file, weights_only=True)
3060  3061          random.setstate(checkpoint_rng_state["python"])
3061  3062          np.random.set_state(checkpoint_rng_state["numpy"])
3062  3063          torch.random.set_rng_state(checkpoint_rng_state["cpu"])
```

Comments 0

Please sign in to comment.