

# AutoDrive Defects and Vulnerability Report

Jianjie Liu, Michael Morscher

Here we are conducting a static analysis of our source code and search of vulnerabilities in our software dependencies. For the static analysis, we use both pylint and pep8. The results are as follow:

```
#####Linting Output - pep8#####
19,1,E,E302:expected 2 blank lines, found 1
33,80,E,E501:line too long (83 > 79 characters)
37,80,E,E501:line too long (84 > 79 characters)
42,27,W,W292:no newline at end of file
```

```
Starting Jedi Python language engine.
#####Linting Output - pylint#####

-----
Your code has been rated at 10.00/10 (previous run: 10.00/10, +0.00)
```

Overall the linting reports show very little problems. However, we identify a high severity issue within our dependencies through GitHub.

pyyaml

Dismiss ▾

 [Open](#) GitHub opened this alert on Jan 4

1 pyyaml vulnerability found in requirements.txt on Jan 4


## Remediation

Upgrade **pyyaml** to version **4.2b1** or later. For example:

```
pyyaml>=4.2b1
```

*Always verify the validity and compatibility of suggestions with your codebase.*

## Details

**CVE-2017-18342** 

high severity

Vulnerable versions: < 4.2b1

Patched version: 4.2b1

In PyYAML before 4.1, the `yaml.load()` API could execute arbitrary code. In other words, `yaml.safe_load` is not used.

We have not directly use this library within our written code and it is mostly involved in the serialization of python objects as a file on disk, or pickle files, which we also have not used. However, we will still update this dependency to the latest version.