Arbitrary code execution via configuration file (.mlrrc) in working directory

High johnkerl published GHSA-mw2v-4q78-j2cw on Sep 1, 2020

Package

miller

Affected versions

5.9.0

Patched versions

5.9.1

Description

Impact

Using the configuration file support introduced in version 5.9.0, it is possible for an attacker to cause Miller to run arbitrary code by placing a malicious `.mlrrc` file in the working directory.

Exemplary attack scenario

A Miller user ...

1. clones a Git repository containing datasets
2. prints one of the files using Miller, e.g via `mlr --c2p cat file.csv`

Their machine now is compromised.

Background and attack details

Since version 5.9.0, Miller supports reading options from one or more configuration files (`.mlrrc`).

The `prepipe` option supports specifying an external command which is executed when Miller processes an input file.

In combination, this makes it possible for an attacker to have Miller execute arbitrary code if they manage to place a `.mlrrc` file into the directory inside which `mlr` is run. By constructing the attacking command suitably, it is even possible to hide the attack, i.e. the input file is passed to `mlr` and processed as normal (see example below).

Example `.mlrrc` file:

```
prepipe touch you_were_attacked; cat
```

Example `mlr` call - user's point of view:

```
$ ls
test.csv

$ mlr --c2p cat test.csv
a b
1 2
3 4

$ ls
test.csv  you_were_attacked
```

Example `mlr` call - showing all files:

```
$ ls -A
.mlrrc  test.csv

$ cat .mlrrc
prepipe touch you_were_attacked; cat

$ mlr --c2p cat test.csv
a b
1 2
3 4

$ ls -A
.mlrrc  test.csv  you_were_attacked
```

The trailing `; cat` in the `prepipe` option causes the input file to be passed through, thus hiding the attack.

In this example, the "attack" simply created a file for demonstration purposes; for a real attack, it is possible for example to instead download a script via the network and run it. For as long as the download and execution of the script do not generate any output, it is again possible to hide the attack as shown above. This was successfully tested with a local web server.

Patches

The fix is in Miller 5.9.1.

Workarounds

As a workaround, you may set the `MLRRC` environment variable to the path of a file which is readable by `mlr` . An empty file is sufficient, but due to a bug which also is fixed in version 5.9.1, the referenced file *must be readable* by `mlr` .

References

See the 5.9.1 release at https://github.com/johnkerl/miller/tree/v5.9.1

For more information

If you have any questions or comments about this advisory:

- Open an issue in johnkerl/miller

Severity

High

CVE ID

CVE-2020-15167

Weaknesses

No CWEs

Credits

koernepr