Relative path traversal vulnerability allows TZInfo::Timezone.get to load arbitrary files

High philr published GHSA-5cm2-9h8c-rvfx on Jul 19

Package

tzinfo (RubyGems)

Affected versions	Patched versions
< 0.3.61	0.3.61
>= 1.0.0, < 1.2.10	1.2.10

Description

Impact

Affected versions

- 0.3.60 and earlier.
- 1.0.0 to 1.2.9 when used with the Ruby data source (tzinfo-data).

Vulnerability

With the Ruby data source (the tzinfo-data gem for tzinfo version 1.0.0 and later and built-in to earlier versions), time zones are defined in Ruby files. There is one file per time zone. Time zone files are loaded with `require` on demand. In the affected versions, `TZInfo::Timezone.get` fails to validate time zone identifiers correctly, allowing a new line character within the identifier. With Ruby version 1.9.3 and later, `TZInfo::Timezone.get` can be made to load unintended files with `require`, executing them within the Ruby process.

For example, with version 1.2.9, you can run the following to load a file with path `/tmp/payload.rb`:

```
TZInfo::Timezone.get("foo\n/../../../../../../../../../../../../../../../../../../../../../tmp/payload")
```

The exact number of parent directory traversals needed will vary depending on the location of the tzinfo-data gem.

TZInfo versions 1.2.6 to 1.2.9 can be made to load files from outside of the Ruby load path. Versions up to and including 1.2.5 can only be made to load files from directories within the load path.

This could be exploited in, for example, a Ruby on Rails application using tzinfo version 1.2.9, that allows file uploads and has a time zone selector that accepts arbitrary time zone identifiers. The CVSS score and severity have been set on this basis.

Versions 2.0.0 and later are not vulnerable.

Patches

Versions 0.3.61 and 1.2.10 include fixes to correctly validate time zone identifiers (commit `9eddbb5` for 0.3.x and commit `9905ca9` for 1.2.x).

Note that version 0.3.61 can still load arbitrary files from the Ruby load path if their name follows the rules for a valid time zone identifier and the file has a prefix of `tzinfo/definition` within a directory in the load path. For example if `/tmp/upload` was in the load path, then `TZInfo::Timezone.get('foo')` could load a file with path `/tmp/upload/tzinfo/definition/foo.rb`. Applications should ensure that untrusted files are not placed in a directory on the load path.

Workarounds

As a workaround, the time zone identifier can be validated before passing to `TZInfo::Timezone.get` by ensuring it matches the regular expression `\A[A-Za-z0-9+\-_]+(?:\/[A-Za-z0-9+\-_]+)*\z`.

For more information

If you have any questions or comments about this advisory:

- Open an issue in the tzinfo repository.

Severity

High 7.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	High

Integrity	**High**
Availability	**High**

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE ID

CVE-2022-31163

Weaknesses

CWE-23 CWE-625 CWE-641

Credits

 **kratob**