jordansissel / **ruby-arr-pm** Public

Code Issues 3 Pull requests 5 Actions Projects Wiki ...

Arbitrary shell execution when extracting or listing files contained in a malicious rpm.

High **jordansissel** published **GHSA-88cv-mj24-8w3q** on Sep 19

Package

arr-pm (RubyGems)

Affected versions	Patched versions
<=0.0.11	0.0.12

Description

Impact

Arbitrary shell execution is possible when using RPM::File#files and RPM::File#extract if the RPM contains a malicious "payload compressor" field.

This vulnerability impacts the `extract` and `files` methods of the `RPM::File` class in the affected versions of this library.

Patches

Version 0.0.12 is available with a fix for these issues.

Workarounds

When using an affected version of this library (arr-pm), ensure any RPMs being processed contain valid/known payload compressor values. Such values include: gzip, bzip2, xz, zstd, and lzma.

You can check the payload compressor field in an rpm by using the rpm command line tool. For example:

```
% rpm -qp example-1.0-1.x86_64.rpm --qf "%{PAYLOADCOMPRESSOR}\n"
gzip
```

Impact on known dependent projects

This library is used by fpm. The vulnerability may impact fpm only when using the flag `-s rpm` or `--input-type rpm` to convert a malicious rpm to another format. It does not impact creating rpms.

References

- #14
- #15

Credit

Thanks to **@joernchen** for reporting this problem and contributing to the resolution :)

For more information

If you have any questions or comments about this advisory:

- Open an issue in the arr-pm issue tracker

Severity

High 7.0 / 10

CVSS base metrics

Attack vector	Local
Attack complexity	High
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

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

CVE ID

CVE-2022-39224

Weaknesses

No CWEs

No CWEs

Credits

joernchen