



# CVE-2022-39224

Published on: Not Yet Published

Last Modified on: 09/26/2022 01:41:00 PM UTC

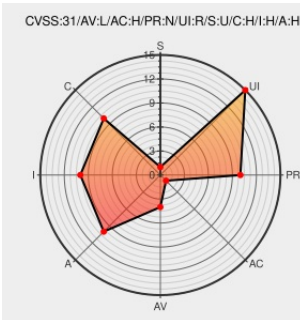
## CVE-2022-39224 - advisory for GHSA-88cv-mj24-8w3q

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Ruby-arr-pm](#) from [Ruby-arr-pm Project](#) contain the following vulnerability:

Arr-pm is an RPM reader/writer library written in Ruby. Versions prior to 0.0.12 are subject to OS command injection resulting in shell execution if the RPM contains a malicious "payload compressor" field. This vulnerability impacts the `extract` and `files` methods of the `RPM::File` class of this library. Version 0.0.12 patches these issues. A workaround

for this issue is to ensure any RPMs being processed contain valid/known payload compressor values such as gzip, bzip2, xz, zstd, and lzma. The payload compressor field in an rpm can be checked by using the rpm command line tool.

CVE-2022-39224 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: jordansissel - [ruby-arr-pm](#) version < 0.0.12

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>LOCAL</b>	<b>LOW</b>	<b>NONE</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

### CVE References

Description	Tags	Link
Only attempt extraction if a known payload compressor is used. by jordansissel · Pull Request #15 · jordansissel/ruby-arr-pm · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="#">github.com/jordansissel/ruby-arr-pm/pull/15</a>
Refactor RPM::File#files by jordansissel · Pull Request #14 · jordansissel/ruby-arr-pm · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="#">github.com/jordansissel/ruby-arr-pm/pull/14</a>
Arbitrary shell execution when extracting or listing files contained in a malicious rpm. · Advisory · jordansissel/ruby-arr-pm · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="#">github.com/jordansissel/ruby-arr-pm/security/advisories/GHSA-88cv-mj24-8w3q</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).






There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Ruby-arr-pm Project</a>	<a href="#">Ruby-arr-pm</a>	All	All	All	All
<code>cpe:2.3:a:ruby-arr-pm_project:ruby-arr-pm:*:*:*:*:ruby:*:*:</code>						

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-39224 : Arr-pm is an RPM reader/writer library written in Ruby. Versions prior to 0.0.12 are subject to OS... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-09-21 23:15:09
 @Inceptus3	New Vulnerability: CVE-2022-39224 #InceptusSecure #UnderOurProtection	2022-09-22 00:20:27
 @LinInfoSec	Ruby - CVE-2022-39224: <a href="https://github.com/jordansissel/r...">github.com/jordansissel/r...</a>	2022-09-22 01:00:26
 @rubylandnews	RubySec → CVE-2022-39224 (arr-pm): arr-pm vulnerable to arbitrary shell execution when extracting or listing... <a href="https://rubysec.com/advisories/CVE...">rubysec.com/advisories/CVE...</a>	2022-09-22 07:20:32
 /r/netcve	<a href="#">CVE-2022-39224</a>	2022-09-22 00:38:15

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**