



CVE-2022-39238

Published on: Not Yet Published

Last Modified on: 09/26/2022 04:35:00 PM UTC

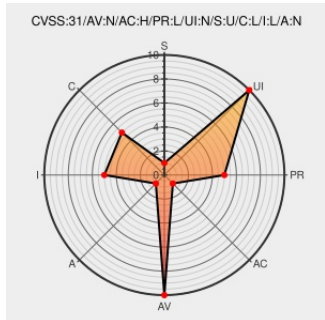
CVE-2022-39238 - advisory for GHSA-87jr-xwhg-cxjv

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Arvados](#) from [Arvados](#) contain the following vulnerability:

Arvados is an open source platform for managing and analyzing biomedical big data. In versions prior to 2.4.3, when using Portable Authentication Modules (PAM) for user authentication, if a user presented valid credentials but the account is disabled or otherwise not allowed to access the host (such as an expired password), it would still be accepted for access to Arvados. Other authentication methods (LDAP, OpenID Connect) supported by Arvados are not affected by this flaw. This issue is patched in version 2.4.3. Workaround for this issue is to migrate to a different authentication method supported by Arvados, such as LDAP.

CVE-2022-39238 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **arvados** - arvados version < 2.4.3

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Improper Authentication in Arvados when using PAM as identity provider · Advisory · arvados/arvados · GitHub	github.com text/html	CONFIRM github.com/arvados/arvados/security/advisories/GHSA-87jr-xwhg-cxjv

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.




There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arvados	Arvados	All	All	All	All
<code>cpe:2.3:a:arvados:arvados:*:*:*:*:ruby:*:*</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-39238 : Arvados is an open source platform for managing and analyzing biomedical big data. In versions pri... twitter.com/i/web/status/1...	2022-09-23 08:11:42
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-39238 Arvados is an open source platform for managing and analyzing bio... twitter.com/i/web/status/1...	2022-09-23 08:56:01
 /r/netcve	CVE-2022-39238	2022-09-23 09:38:06

[← 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