



CVE-2022-36006

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-36006
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-15 11:21:00 UTC
Updated	2023-06-29 16:18:00 UTC
Description	Arvados is an open source platform for managing, processing, and sharing genomic and other large scientific and biomedical data. This vulnerability allows an attacker to execute arbitrary code on the host system by exploiting a buffer overflow in the Arvados API. The vulnerability is located in the Arvados API, specifically in the /api/v1/containers endpoint. The issue is caused by a buffer overflow in the Arvados API, which allows an attacker to execute arbitrary code on the host system by exploiting a buffer overflow in the Arvados API. The vulnerability is located in the Arvados API, specifically in the /api/v1/containers endpoint. The issue is caused by a buffer overflow in the Arvados API, which allows an attacker to execute arbitrary code on the host system by exploiting a buffer overflow in the Arvados API.

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arvados	Arvados	All	All	All	All

References

Reference	Source
Bug #19316: Audit usage of Oj gem & make sure to use safe_load or replace with different gem - Arvados	MISC
Authenticated remote code execution due to insecure deserialization (GHSL-2022-063) · Advisory · arvados/arvados · GitHub	CONFIRM
Arvados 2.4.2 Release Notes Arvados	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report