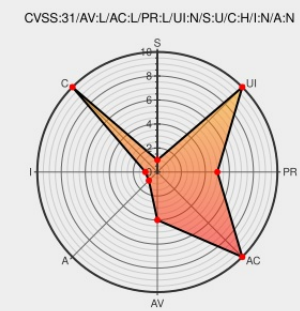
CVE-2023-2782

Published on: Not Yet Published

Last Modified on: 05/25/2023 04:23:00 PM UTC

CVE-2023-2782

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cyber Infrastructure from Acronis contain the following vulnerability:

Sensitive information disclosure due to improper authorization. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.3.1-38.

CVE-2023-2782 has been assigned by security@acronis.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Acronis** - **Acronis Cyber Infrastructure** version **< 5.3.1-38**

CVSS3 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
Acronis Advisory Database - Acronis	security-advisory.acronis.com text/html	MISC security-advisory.acronis.com/advisories/SEC-3475

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acronis	Cyber Infrastructure	All	All	All	All

cpe:2.3:a:acronis:cyber_infrastructure:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-2782 : Sensitive information disclosure due to improper authorization. The following products are affected… twitter.com/i/web/status/1…	2023-05-18 11:05:11

← Previous ID

Next ID→