



CVE-2021-41137

Published on: 10/13/2021 12:00:00 AM UTC

Last Modified on: 10/19/2021 03:08:00 PM UTC

CVE-2021-41137 - advisory for GHSA-v64v-g97p-577c

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



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

Minio is a Kubernetes native application for cloud storage. All users on release `RELEASE.2021-10-10T16-53-30Z` are affected by a vulnerability that involves bypassing policy restrictions on regular users. Normally, `checkKeyValid()` should return `owner true` for `rootCreds`. In the affected version, policy restriction did not work properly for users who did not have service (svc) or security token

service (STS) accounts. This issue is fixed in `RELEASE.2021-10-13T00-23-17Z`. A downgrade back to release `RELEASE.2021-10-08T23-58-24Z` is available as a workaround.

CVE-2021-41137 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **minio** - minio version = **RELEASE.2021-10-10T16-53-30Z**

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 |

CVSS2 Score: **6.5 - MEDIUM**

| Access Vector | Access Complexity | Authentication |
|------------------------|-------------------|---------------------|
| NETWORK | LOW | SINGLE |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| PARTIAL | PARTIAL | PARTIAL |

CVE References

| Description | Tags | Link |
|--|---|--|
| checkKeyValid() should return owner true for rootCreds (#13422) · minio/minio@415bbc7 · GitHub | github.com text/html | MISC github.com/minio/minio/commit/415bbc74aacd53a120e54a663e941b1809982dbd |
| Bypassing policy restrictions on regular users · Advisory · minio/minio · GitHub | github.com text/html | CONFIRM github.com/minio/minio/security/advisories/GHSA-v64v-g97p-577c |
| fix: disallow invalid x-amz-security-token for root credentials by harshavardhana · Pull Request #13388 · minio/minio · GitHub | github.com text/html | MISC github.com/minio/minio/pull/13388 |
| checkKeyValid() should return owner true for rootCreds by harshavardhana · Pull Request #13422 · minio/minio · GitHub | github.com text/html | MISC github.com/minio/minio/pull/13422 |

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 | Minio | Minio | 2021-10-10t16-53-30z | All | All | All |
| <code>cpe:2.3:a:minio:minio:2021-10-10t16-53-30z:*:*:*:*:*:</code> | | | | | | |

No vendor comments have been submitted for this CVE

Social Mentions

| Source | Title | Posted (UTC) |
|------------|--|---------------------|
| @CVEreport | CVE-2021-41137 : Minio is a Kubernetes native application for cloud storage. All users on release `RELEASE.2021-10-... twitter.com/i/web/status/1... | 2021-10-13 14:06:26 |
| @InakMali | #CVE-2021-41137 affecting @Minio #Kubernetes detected. | 2021-10-13 14:48:32 |

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021 |

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