



# CVE-2022-24842

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

## Summary

<b>CVE</b>	CVE-2022-24842
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-12 18:15:00 UTC
<b>Updated</b>	2023-07-06 13:51:00 UTC
<b>Description</b>	MinIO is a High Performance Object Storage released under GNU Affero General Public License v3.0. A security issue was

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

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

## References

Reference	Source	Link
Fix service account privilege escalation by donatello · Pull Request #14729 · minio/minio · GitHub	MISC	<a href="#">github.com</a>
Fix service account privilege escalation (#14729) · minio/minio@66b14a0 · GitHub	MISC	<a href="#">github.com</a>
Unprivileged user is able to create service accounts for root or other admin users · Advisory · minio/minio · GitHub	CONFIRM	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[691063](#) Free Berkeley Software Distribution (FreeBSD) Security Update for minio (8e20430d-a72b-11ed-a04f-40b034455553)

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](#)**