



CVE-2022-35919

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

Summary

CVE	CVE-2022-35919
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-01 22:15:00 UTC
Updated	2023-10-10 17:15:00 UTC
Description	MinIO is a High Performance Object Storage released under GNU Affero General Public License v3.0. In affected versions

Risk And Classification

Problem Types: CWE-22

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
Authenticated requests for server update admin API allows path traversal · Advisory · minio/minio · GitHub	CONFIRM	github.com
Minio 2022-07-29T19-40-48Z Path Traversal ≈ Packet Storm	MISC	packetstorm.com
do not allow filesystem fallback in server download (#15429) · minio/minio@bc72e42 · GitHub	MISC	github.com
do not allow filesystem fallback in server download by harshavardhana · Pull Request #15429 · minio/minio · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)