

CVE-2023-28432

MinIO Information Disclosure Vulnerability

CISA KEV since Apr 21, 2023

Actively exploited

Public exploit module (Metasploit)

Minio is a Multi-Cloud Object Storage framework. In a cluster deployment starting with RELEASE.2019-12-17T23-16-33Z and prior to RELEASE.2023-03-20T20-16-18Z, MinIO returns all environment variables, including `MINIO\_SECRET\_KEY` and `MINIO\_ROOT\_PASSWORD`, resulting in information disclosure. All users of distributed deployment are impacted. All users are advised to upgrade to RELEASE.2023-03-20T20-16-18Z.

EVRS 80/₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.840 99.69th percentile · FIRST	CISA DEADLINE May 12, 2023 KEV since 2023 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.840 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
minio	≥ 2019-12-17t23-16-33z < 2023-03-20t20-16-18z	2023-03-20t20-16-18z	NVD

Sources

Vendor guidance	github.com/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q	NVD	nvd.nist.gov/vuln/detail/CVE-2023-28432
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-32124
Current data	evulnable.com/vulnerability-management/cve/CVE-2023-28432		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.