مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High Severity Vulnerability in MinIO Vulnerability

Tracking #:432317042

Date:07-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity vulnerability (CVE-2025-31489) has been identified in MinIO, an open-source object storage solution compatible with Amazon S3.

TECHNICAL DETAILS:

A high-severity vulnerability has been identified in MinIO, an open-source object storage solution compatible with Amazon S3. The vulnerability, tracked as CVE-2025-31489, stems from incomplete signature validation for unsigned-trailer uploads. This flaw allows malicious actors to upload unauthorized objects to buckets, potentially leading to data compromise and security breaches. Exploiting this vulnerability requires WRITE permissions on the bucket, knowledge of the access key, and the bucket name. MinIO has urgently released a patch to address this issue, and all users are strongly advised to upgrade immediately to the patched version

Vulnerability Details

- **CVE ID: CVE-2025-31489**
- **Severity:** High
- **Affected Product:** MinIO Object Storage Server
- **Impacted Version:** RELEASE.2023-05-18T00-05-36Z
- **Patched Version:** RELEASE.2025-04-03T14-56-28Z
- **Exploitability:** Requires:
  - Valid access key
  - Bucket name
  - Prior WRITE permissions

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade MinIO to fixed version or later without delay.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/minio/minio/security/advisories/GHSA-wg47-6jq2-q2hh