مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in MinIO

Tracking #:432317835

Date:20-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a privilege escalation vulnerability in MinIO that allows attackers to bypass session policy restrictions via service and STS accounts, potentially enabling unauthorized access, modification, or deletion of restricted data.

TECHNICAL DETAILS:

MinIO, a widely used high-performance, S3-compatible object storage platform, have identified a privilege escalation vulnerability that could allow attackers to bypass session policy restrictions and gain elevated permissions through service accounts and Security Token Service (STS) tokens.

Successful exploitation could enable unauthorized users to access, modify, or delete data across restricted buckets, posing a significant risk to the confidentiality and integrity of stored information in cloud and enterprise environments.

Vulnerability Details

- CVE-2025-62506
- CVSS Score 8.1 High
- The vulnerability exists in MinIO's IAM policy validation logic (cmd/iam.go). During validation, the system incorrectly relied on the DenyOnly parameter, allowing restricted session policies to bypass proper access checks. As a result, service or STS accounts with limited permissions could create new service accounts without restrictions, inheriting full privileges from the parent user.

Impact:

Attackers with valid restricted credentials could:

- Escalate privileges by creating unrestricted service accounts
- Access, modify, or delete data across unauthorized buckets
- Compromise confidentiality and integrity of stored information

Affected Versions

- All MinIO versions **prior to** RELEASE.2025-10-15T17-29-55Z are affected.

Fixed Version

- **Patched Release:** RELEASE.2025-10-15T17-29-55Z

RECOMMENDATIONS:

- Upgrade MinIO: Apply the latest release containing the patch.
- Audit Service Accounts: Verify that all non-admin accounts comply with privilege restrictions.
- Revoke Suspicious Accounts: Remove unauthorized or unrestricted service accounts.
- Review access logs for unusual activity across sensitive buckets.

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://nvd.nist.gov/vuln/detail/CVE-2025-62506