New issue

Jump to bottom

Fix service account privilege escalation #14729

Merged

harshavardhana merged 1 commit into `minio:master` from `donatello:fix-svc-acc-priv-escalation` on Apr 11

donatello commented on Apr 11 • edited

Member

Description

- Ensure that a regular unprivileged user is unable to create service accounts for other users/root.

This fix includes tests to check this scenario is not possible.

Motivation and Context

Fixes a security issue where an unprivileged user is able to create service accounts for root or other user and then is able to assume their access policies via the generated credentials.

This is a regression that has existed since version RELEASE.2021-12-09T06-19-41Z.

How to test this PR?

```
mc admin user add myminio foo foobar123
mc admin policy set myminio readonly user=foo
MC_HOST_foo=http://foo:foobar123@localhost:9000 mc admin user svcacct add foo someOtherUser
```

The last command above should fail.

Types of changes

- [x] Bug fix (non-breaking change which fixes an issue)

- [ ] New feature (non-breaking change which adds functionality)
- [ ] Optimization (provides speedup with no functional changes)
- [ ] Breaking change (fix or feature that would cause existing functionality to change)

Checklist:

- [x] Fixes a regression (introduced in Fix LDAP service account creation #13849)
- [ ] Documentation updated
- [x] Unit tests added/updated

`Fix service account privilege escalation` ... ✓ `f0daa65`

donatello added priority: high priority: severe regression fixed and removed priority: high labels on Apr 11

donatello requested review from **harshavardhana**, **vadmeste**, **krisis** and **kannappanr** 8 months ago

donatello added priority: high and removed priority: severe labels on Apr 11

harshavardhana approved these changes on Apr 11

View changes

harshavardhana commented on Apr 11 — Member

Will open a security tracker for this **@donatello**

donatello commented on Apr 11 — Member Author

> Will open a security tracker for this **@donatello**

Ack

minio-trusted commented on Apr 11 — Contributor

Mint Automation

Test	Result
mint-large-bucket.sh	✔
mint-fs.sh	✔
mint-gateway-s3.sh	✔
mint-erasure.sh	✔
mint-dist-erasure.sh	✔
mint-gateway-nas.sh	✔
mint-compress-encrypt-dist-erasure.sh	✔
mint-pools.sh	✔
Deleting image on docker hub	
Deleting image locally	

kannappanr approved these changes on Apr 11

View changes

vadmeste approved these changes on Apr 11

View changes

vadmeste left a comment — Member

LGTM

harshavardhana merged commit `66b14a0` into `minio:master` on Apr 11

13 checks passed

View details

donatello deleted the `fix-svc-acc-priv-escalation` branch 8 months ago

GoVulnBot mentioned this pull request on Apr 12

x/vulndb: potential Go vuln in github.com/minio/minio: CVE-2022-24842

golang/vulndb#421

Closed

vadmeste pushed a commit to vadmeste/minio that referenced this pull request on May 5

`Fix service account privilege escalation (minio#14729)` ... `96c1cfe`

Reviewers

- vadmeste ✓
- harshavardhana ✓
- kannappanr ✓
- krisis ●

Assignees

No one assigned

Labels

priority: high regression fixed

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

5 participants