minio / **minio** Public

<> Code   Issues 18   Pull requests 16   Discussions   Actions   **Security** 9 •••

Authenticated requests for server update admin API allows path traversal

High **minio-trusted** published **GHSA-gr9v-6pcm-rqvg** on Jul 29

Package

minio (Go)

Affected versions	Patched versions
>= RELEASE.2020-07-24T22-43-05Z	RELEASE.2022-07-29T19-40-48Z

Description

Impact

All 'admin' users authorized for `admin:ServerUpdate` can selectively trigger an error that in response, in turn, returns the content of the path requested for example

```
mc admin update alias/ /etc/passwd
```

The contents of `/etc/passwd` are returned back with an error response, so any normal OS system would allow access to contents at any arbitrary paths that are readable by MinIO process.

This issue was discovered by **@Alevsk** during an internal security audit. The affected code has been removed from the repository.

Patches

```
commit bc72e4226e669d98c8e0f3eccc9297be9251c692
Author: Harshavardhana <harsha@minio.io>
Date:   Thu Jul 28 17:44:21 2022 -0700

    do not allow filesystem fallback in server download (#15429)

    It is possible for anyone with admin access to relatively
    to get any content of any random OS location by simply
```

```
      providing the file with 'mc admin update alias/ /etc/passwd`.

      Workaround is to disable 'admin:ServiceUpdate' action. Everyone
      is advised to upgrade to this patch.

      Thanks to @alevsk for finding this bug.
```

Workarounds

You can disable ServerUpdate API by denying the `admin:ServerUpdate` action for your admin users via IAM policies.

For example an explicit "Deny" for "admin:ServerUpdate" until you can upgrade the affected systems to the latest releases.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "admin:*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "admin:ServerUpdate"
      ]
    }
  ]
}
```

References

The referenced PR #15429 provides the relevant details

For more information

If you have any questions or comments about this advisory:

- Open an issue in issues
- Email us at security@min.io

Severity

High

CVE ID

CVE-2022-35919

Weaknesses

No CWEs

Credits

Alevsk