New issue

Jump to bottom

s3v4: read and verify S3 signature v4 chunks separately #11801

Merged harshavardhana merged 1 commit into minio:master from aead:signature-v4-stream on Mar 16, 2021

aead commented on Mar 16, 2021 Member

Description

This commit fixes a security issue in the signature v4 chunked reader. Before, the reader returned unverified data to the caller and would only verify the chunk signature once it has encountered the end of the chunk payload.

Now, the chunk reader reads the entire chunk into an in-memory buffer, verifies the signature and then returns data to the caller.

In general, this is a common security problem. We verifying data streams, the verifier MUST NOT return data to the upper layers / its callers as long as it has not verified the current data chunk / data segment:

```
func (r *Reader) Read(buffer []byte) {
   if err := r.readNext(r.internalBuffer); err != nil {
      return err
   }
   if err := r.verify(r.internalBuffer); err != nil {
      return err
   }
   copy(buffer, r.internalBuffer)
}
```

Motivation and Context

Signature V4, Security

How to test this PR?

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:

- [ ] Fixes a regression (If yes, please add `commit-id` or `PR #` here)
- [ ] Documentation updated
- [ ] Unit tests added/updated

harshavardhana added the priority: high label on Mar 16, 2021

harshavardhana approved these changes on Mar 16, 2021

View changes

s3v4: read and verify S3 signature v4 chunks separately ... 9abf187

aead force-pushed the signature-v4-stream branch from 394cc2c to 9abf187 last year Compare

minio deleted a comment from minio-trusted on Mar 16, 2021

aead requested a review from Alevsk last year

minio-trusted commented on Mar 16, 2021 Contributor

Mint Automation

Test	Result
mint-large-bucket.sh	✓
mint-fs.sh	✓
mint-gateway-s3.sh	✓
mint-erasure.sh	✓
mint-dist-erasure.sh	✓
mint-zoned.sh	✓
mint-gateway-nas.sh	✓
mint-compress-encrypt-dist-erasure.sh	✗ more...

11801-9abf187/mint-compress-encrypt-dist-erasure.sh.log:

```
Running with
SERVER_ENDPOINT:      minio-c2.minio.io:31079
ACCESS_KEY:           minio
SECRET_KEY:           ***REDACTED***
ENABLE_HTTPS:         0
SERVER_REGION:        us-east-1
MINT_DATA_DIR:        /mint/data
MINT_MODE:            full
ENABLE_VIRTUAL_STYLE: 0

To get logs, run 'docker cp 3965745049c2:/mint/log /tmp/mint-logs'

(1/15) Running aws-sdk-go tests ... done in 2 seconds
(2/15) Running aws-sdk-java tests ... done in 1 seconds
(3/15) Running aws-sdk-php tests ... done in 43 seconds
(4/15) Running aws-sdk-ruby tests ... done in 5 seconds
(5/15) Running awscli tests ... FAILED in 33 seconds
{
  "name": "awscli",
  "duration": 2640,
  "function": "aws --endpoint-url http://minio-c2.minio.io:31079 s3api copy-object --bucket awscli-mint-test-bucket-18011 --key datafile-1-kB-copy --copy-source awscli-mint-test-
bucket-18011/datafile-1-kB\n",
  "status": "FAIL",
  "error": "Hash mismatch expected 084e1383b70fb0c51acc680fef370023, got ac57de7156d7fc25ac1a65f81fa3989b"
}
(5/15) Running healthcheck tests ... done in 0 seconds
(6/15) Running mc tests ... done in 48 seconds
(7/15) Running minio-dotnet tests ... done in 43 seconds
(8/15) Running minio-go tests ... FAILED in 2 minutes and 26 seconds
{
  "args": {},
  "duration": 279,
  "error": "At least one of the pre-conditions you specified did not hold",
  "function": "CopyObjectPart(destination, source)",
  "message": "CopyObjectPart call failed",
  "name": "minio-go: testUnencryptedToSSES3CopyObjectPart",
  "status": "FAIL"
}
(8/15) Running minio-java tests ... FAILED in 1 minutes and 52 seconds
{
  "name": "minio-java",
  "function": "copyObject()",
  "args": "[match etag]",
  "duration": 389,
  "status": "FAIL",
  "error": "error occurred\nErrorResponse(code = PreconditionFailed, message = At least one of the pre-conditions you specified did not hold, bucketName = minio-java-test-1r4veli,
objectName = minio-java-test-1kvhidu-copy, resource = /minio-java-test-1r4veli/minio-java-test-1kvhidu-copy, requestId = 166CE72B61205B18, hostId = 241226af-b142-4af9-ba37-
f8f3f9bac301)\nrequest={method=PUT, url=http://minio-c2.minio.io:31079/minio-java-test-1r4veli/minio-java-test-1kvhidu-copy, headers=x-amz-copy-source-if-match:
71cff0a060f852067e443ad1e24ae26c-1\nx-amz-copy-source: /minio-java-test-1hr2jbr/minio-java-test-1kvhidu\nHost: minio-c2.minio.io:31079\nAccept-Encoding: identity\nUser-Agent: MinIO
(Linux; amd64) minio-java/8.0.3\nContent-MD5: 1B2M2Y8AsgTpgAmY7PhCfg==\nx-amz-content-sha256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855\nx-amz-date:
20210316T184859Z\nAuthorization: AWS4-HMAC-SHA256 Credential=*REDACTED*/20210316/us-east-1/s3/aws4_request, SignedHeaders=content-md5;host;x-amz-content-sha256;x-amz-copy-source;x-
amz-copy-source-if-match;x-amz-date, Signature=*REDACTED*\n}\nresponse={code=412, headers=Accept-Ranges: bytes\nContent-Length: 418\nContent-Security-Policy: block-all-mixed-
content\nContent-Type: application/xml\nETag: \"71cff0a060f852067e443ad1e24ae26c\"\nLast-Modified: Tue, 16 Mar 2021 18:48:59 GMT\nServer: MinIO\nVary: Origin\nX-Amz-Request-Id:
166CE72B61205B18\nX-Xss-Protection: 1; mode=block\nDate: Tue, 16 Mar 2021 18:48:59 GMT\n}\n >>> [io.minio.MinioClient.execute(MinioClient.java:775),
io.minio.MinioClient.execute(MinioClient.java:563), io.minio.MinioClient.executePut(MinioClient.java:904), io.minio.MinioClient.copyObject(MinioClient.java:1232),
FunctionalTest.testCopyObjectMatchETag(FunctionalTest.java:1850), FunctionalTest.copyObject(FunctionalTest.java:2016), FunctionalTest.runObjectTests(FunctionalTest.java:3757),
FunctionalTest.runTests(FunctionalTest.java:3783), FunctionalTest.main(FunctionalTest.java:3927)]"
}
(8/15) Running minio-js tests ... done in 52 seconds
(9/15) Running minio-py tests ... done in 3 minutes and 30 seconds
(10/15) Running s3cmd tests ... FAILED in 5 seconds
{
  "name": "s3cmd",
  "duration": "2731",
  "function": "test_put_object_multipart",
  "status": "FAIL",
  "error": "WARNING: MD5 Sums don't match!\nWARNING: Retrying upload of /mint/data/datafile-65-MB\nWARNING: MD5 Sums don't match!\nWARNING: Retrying upload of /mint/data/datafile-
65-MB\nWARNING: MD5 Sums don't match!\nWARNING: Retrying upload of /mint/data/datafile-65-MB\nWARNING: MD5 Sums don't match!\nWARNING: Retrying upload of /mint/data/datafile-65-
MB\nWARNING: MD5 Sums don't match!\nWARNING: Retrying upload of /mint/data/datafile-65-MB\nWARNING: MD5 Sums don't match!\nWARNING: Too many failures. Giving up on
'/mint/data/datafile-65-MB'\nERROR: \nUpload of '/mint/data/datafile-65-MB' part 1 failed. Use\n  /usr/local/bin/s3cmd abortmp s3://s3cmd-test-bucket-10925/s3cmd-test-object-0
8cc397aa-d899-45c4-9953-acb4a940e638\nto abort the upload, or\n  /usr/local/bin/s3cmd --upload-id 8cc397aa-d899-45c4-9953-acb4a940e638 put ...\nto continue the upload.\nERROR:
Upload of '/mint/data/datafile-65-MB' failed too many times (Last reason: )"
}
(10/15) Running s3select tests ... done in 9 seconds
(11/15) Running security tests ... done in 0 seconds

Executed 11 out of 15 tests successfully.
```

Deleting image on docker hub
Deleting image locally

Alevsk approved these changes on Mar 16, 2021

View changes

Alevsk left a comment — Contributor

LGTM

harshavardhana merged commit `e197800` into `minio:master` on Mar 16, 2021

3 checks passed

View details

igsol mentioned this pull request on Sep 8, 2021

Internal error, malformed chunked encoding #13163

Closed

1 task

Reviewers

harshavardhana ✓

Alevsk ✓

Assignees

No one assigned

Labels

priority: high

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

4 participants