Chunked body signature check not always applied

Moderate **harshavardhana** published **GHSA-xr7r-7gpj-5pgp** on Mar 16, 2021

Package

MinIO

Affected versions	Patched versions
< RELEASE.2021-03-17T02-33-02Z	RELEASE.2021-03-17T02-33-02Z

Description

Impact

This is a security issue because it enables MITM modification of request bodies that are meant to have integrity guaranteed by chunk signatures.

In a PUT request using aws-chunked encoding, MinIO ordinarily verifies signatures at the end of a chunk. This check can be skipped if the client sends a false chunk size that is much greater than the actual data sent: the server accepts and completes the request without ever reaching the end of the chunk + thereby without ever checking the chunk signature.

Patches

Patched by **@aead** in PR #11801, users are advised to upgrade to RELEASE.2021-03-17T02-33-02Z

Workarounds

Avoid using "aws-chunked" encoding-based chunk signature upload requests instead use TLS.
MinIO SDKs automatically disable chunked encoding signature when the server endpoint is configured with TLS.

References

#11801 for more information on the fix and how it was fixed.

For more information

If you have any questions or comments about this advisory:

- Open an issue at here
- Email us at security

Severity

Moderate

CVE ID

CVE-2021-21390

Weaknesses

No CWEs

Credits

aead

jcsp