Audacious - OLD, PLEASE USE GITHUB DISCUSSIONS/ISSUES - Bug #1090

Open Containing Folder can open other types of files

April 28, 2021 12:31 - Fabian B

Status:	Closed	**Start date:**	April 28, 2021
Priority:	Major	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	4.2		
Affects version:	4.1		

Description

Hi Team,

As I haven't received a response yet trying to report the vulnerability privately, I decided to now report it via the bug tracker:

1. Description
   The `Playlist Item > Open Containing Folder` menu item, mapping to `pl_open_folder()`, utilizes `QDesktopServices::openUrl()`, which calls the OS'/Desktop environment's default application handler to open the URL.
   By adding a bogus `/filename.mp3` to a playlist item (e.g. `file:///etc/passwd/123), `Open Containing Folder` actually opens the referenced file with its default application.
   Depending on the OS/Desktop environment, this can be exploited to gain code execution when a user opens a malicious playlist and clicks "Open Containing Folder" on an item.
2. Exploitation
   1. Windows
      Setting a playlist item's location to a `.jar` file on an anonymous SMB or DAV share auto-mounts the share and allows execution of arbitrary code. A demo video is attached.
      Besides `.jar`, also other filetypes could be used, with `.exe` files requiring one more confirmation to run. During the establishment of the SMB connection, the user's NTLM hash might also be leaked, allowing for offline-cracking of the password or Pass-the-Hash attacks (but outgoing SMB to the internet might be blocked by a firewall).
   2. Linux
      On Linux, the exact opening behavior and therefore exploitation strategy is dependent on the Desktop Environment and its configuration. On Xubuntu 20.04, opening `nfs://<server>/bitcoin.desktop/` leads to code execution without any additional confirmation (the remote location is auto-mounted and the .desktop file (with executable-flag set) is opened with its default application, which will execute the specified command).
      Testing the payload in Audacious surprisingly did not result in code execution (but a connection to the server was made). I did not spent much time looking into what could be the difference between Audacious' openURL-call and my `xdg-open` tests, but I think it's likely that with further investigation, a working PoC could be crafted (the trailing slash should not be an issue according to my tests).
   3. OS-independent
      In addition to abusing OS-specific URL handing behavior, it's also possible to exploit vulnerabilities in custom URI handling applications, e.g. exploiting CVE-2021-3331 in WinSCP via a malicious "sftp://"-URL. (See attached screenshot, where the mail client is opened due to a "mailto://"-location)
3. Recommendation
   Implement the following validation in `pl_open_folder` before passing the path to openURL:
   - the URI scheme must be `file://`
   - the path must point to a local directory (no remote hostname)
   - ensure the path points to a directory (e.g. using Qt: "QFileInfo(dir_path).isDir()")
4. Background / Credits
   My colleague Lukas and I recently published some research results on the URI handling. You can check our post for more details and examples (including a very similar vulnerability in VLC): https://positive.security/blog/url-open-rce
   After sharing the blog post draft with Hanno Böck, he checked Audacious and sent me the code of the pl_open_folder() function that seemed to include the vulnerable code pattern.

Thank you,
Fabian

History

#1 - April 30, 2021 03:08 - John Lindgren

- Subject changed from Vulnerability - 1-click RCE via malicious playlist entry to Open Containing Folder can open other types of files

Okay - I changed the bug title since it was over-dramatic for a couple reasons:

1. This isn't a "1-click" vulnerability. It would have to be at least 3 clicks: 1) open a malicious playlist URL in Audacious, 2) right-click on an entry in the playlist, and 3) click "Open Containing Folder".

2. From your examples, it seems that this is not a "remote code execution" vulnerability in its own right, but has to be chained to another vulnerability (e.g. auto-mounting an untrusted SMB share without user confirmation) in order to lead to code execution.

However, it's a valid bug since a user would not expect "Open Containing Folder" to open other types of file (such as .jar or .desktop files). So thanks for reporting it. I will have a fix shortly.

#2 - April 30, 2021 03:13 - John Lindgren

I also note that in my tests, `xdg-open` does not open a regular file if a trailing slash is appended to the name. So at least on Linux, this bug is purely theoretical.

#3 - April 30, 2021 03:19 - John Lindgren

- % Done changed from 0 to 100

- Status changed from New to Closed

Fixed:
https://github.com/audacious-media-player/audacious-plugins/commit/bb822846f5fd662904b9b22eb6c4abad36affe34

#4 - April 30, 2021 03:19 - John Lindgren

- Affects version 4.1 added

#5 - April 30, 2021 15:07 - Fabian B

Thanks for your quick response and fix!

#6 - February 05, 2022 22:21 - John Lindgren

- Target version set to 4.2