Attaching files with mailto:?attach=... parameter is considered dangerous
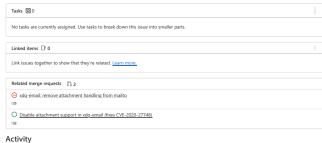
In `run_thunderbird()`, xdg-email greps for a proprietary `attach` parameter: https://gitlab.freedesktop.org/xdg/xdg-utils/-/blob/master/scripts/xdg-email.in#L51

This allows arbitrary websites with mailto links to add local files on disk into the Thunderbird's email composition dialog and should be removed: https://twitter.com/i/status/1295357952480751616

After Thunderbird removed this functionality years ago, I think xdg-email somewhat re-introduced it. Original bug report for Thunderbird: https://bugzilla.mozilla.org/show_bug.cgi?id=1613425

⬆ Drag your designs here or click to upload.

Tasks ◎ 0	

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items ⬚ 0	

Link issues together to show that they're related. Learn more.

Related merge requests ⭢ 2

⊖ xdg-email: remove attachment handling from mailto
!28

○ Disable attachment support in xdg-email (fixes CVE-2020-27748)
!58

Activity

Kai Engert @kaie · 2 years ago
Code was originally added 11 years ago in this commit: 53bd27e8

💬 **Jörg Thalheim** mentioned in commit `Mic92/xdg-utils@1f199813` 2 years ago

💬 **Jörg Thalheim** mentioned in merge request !28 (closed) 2 years ago

Salvatore Bonaccorso @carnil · 2 years ago
CVE-2020-27748 was assigned for this issue.

💬 **Marco Kühnel** mentioned in issue #205 4 months ago

Gabriel Corona @randomstuff · 3 months ago
Indeed, it works with a command such as:

```
xdg-email mailto:foo@example.com?attach=~/.ssh/id_rsa
```

Under certain circumstances, this calls:

```
thunderbird -compose to='foo@example.com',attachment='~/.ssh/id_rsa
```

which triggers the inclusion of the file.

It only works under some circonstances (roughly when using Thunderbird with GNOME or KDE). In my case, this cals:

```
exo-open mailto:foo@example.com?attach=~/.ssh/id_rsa
```

which in turns calls:

```
thunderbird mailto:foo@example.com?attach=~/.ssh/id_rsa
```

In this case Thunderbird does NOT attach file file.

Gabriel Corona @randomstuff · 3 months ago
Could we merge `Mic92/xdg-utils@1f199813` ?

Thunderbird is the only case where attachements are not passed through the mailto URI. But this only works in some cases, depending on the Desktop Environment.

In all other cases, the attachments are passed through the mailto URI and we can expect (hope) that the callee does not honor this parameter.

As a consequence, it appears we should consider the `attachment --attach` functionnality to be non-functional.

💬 **Gabriel Corona** mentioned in merge request !58 3 months ago

Please register or sign in to reply