Accidental removal of IPCPassword (< 5.1.2.4)

Moderate JustArchi published GHSA-wxx4-66c2-vj2v on Jul 23, 2021

Package

ArchiSteamFarm (GitHub)

Affected versions	Patched versions
< 5.1.2.4	≥ 5.1.2.4

Description

Impact

What kind of vulnerability is it? Who is impacted?

Due to a bug in ASF code, resolved as part of #2379, `POST /Api/ASF` ASF API endpoint responsible for updating global ASF config incorrectly removed `IPCPassword` from resulting (updated) config when the caller (e.g. ASF-ui) did not specify it explicitly. This is incorrect behaviour, as existing `IPCPassword` should be preserved in the config itself if the caller does not specify it explicitly. The same behaviour applies to other sensitive properties, e.g. `SteamLogin` or `SteamPassword`, however, the bug described in this security advisory applies only to `IPCPassword` as only that property behaved incorrectly.

Due to the above, it was possible for the user to accidentally remove `IPCPassword` security measure from his IPC interface when updating global ASF config, which exists e.g. as part of global config update functionality in ASF-ui. Removal of `IPCPassword` possesses a security risk, as unauthorized users may in result access the (now insecure) IPC interface after such modification.

It was not possible to remove `IPCPassword` remotely without prior authorization or in any other way access protected IPC interface. Since the authorized user had to run into the bug described here and therefore authorize himself firstly, this issue is not critical, but of significant severity (to be exact, a bug in the program that could lead to security issue rather than security issue itself).

Patches

Has the problem been patched? What versions should users upgrade to?

The issue is patched in ASF V5.1.2.4 and future versions.

While the patch itself will not bring removed `IPCPassword` back, additional security measures implemented as part of ASF V5.1.2.1 and above limit the damage by refusing to handle remote requests without `IPCPassword` set.

We recommend to manually verify that `IPCPassword` is specified after update, and if not, set it accordingly.

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?

In default settings, ASF is configured to allow IPC access from `localhost` **only**, therefore the bug itself has rather very limited scope and should not affect majority of users in any negative way. Of course, the issue doesn't apply whatsoever if somebody is not using `IPC` at all.

In any case, the workaround would be to refrain from using `POST /Api/ASF` (so not using ASF-ui global config update functionality), or manually setting `IPCPassword` again after its removal. Once again, there is no security breach that would allow attacker to execute this bug remotely, it requires properly authorized user modifying the global config first.

References

Are there any links users can visit to find out more?

The issue was originally reported at https://steamcommunity.com/groups/archiasf/discussions/6/3057365873428498659/

The fix was applied as part of #2379

We suspect that the issue described here could be the root cause of reported security incidents mentioned in the thread above, as well as other places such as https://keylol.com/t733938-1-1

For more information

If you have any questions or comments about this advisory:

- Use our **support** channels.

Severity

Moderate 6.8 / 10

CVSS base metrics

Attack vector	Adjacent
Attack complexity	High
Privileges required	Low
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

CVE ID

CVE-2021-32794

Weaknesses

No CWEs

Credits

- Abrynos
- deluxghost
- Botan626
- MrBurrBurr
- JustArchi