



CVE-2021-32794

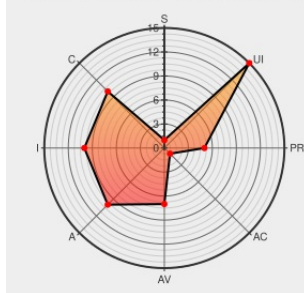
Published on: 07/26/2021 12:00:00 AM UTC

Last Modified on: 07/02/2022 06:30:00 PM UTC

CVE-2021-32794 - advisory for GHSA-wxx4-66c2-vj2v

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Archisteamfarm](#) from [Archisteamfarm Project](#) contain the following vulnerability:

ArchiSteamFarm is a C# application with primary purpose of idling Steam cards from multiple accounts simultaneously. Due to a bug in ASF code ``POST /Api/ASF`` ASF API endpoint responsible for updating global ASF config incorrectly removed ``IPCPassWord`` from the resulting config when the caller did not specify it explicitly. 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 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 IPC interface after such modification. The issue is patched in ASF V5.1.2.4 and future versions. We recommend to manually verify that ``IPCPassWord`` is specified after update, and if not, set it accordingly. In default settings, ASF is configured to allow IPC access from ``localhost`` only and should not affect majority of users.

CVE-2021-32794 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [JustArchiNET](#) - [ArchiSteamFarm](#) version < 5.1.2.4

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description	Tags	Link
Accidental removal of IPCPassword (< 5.1.2.4) · Advisory · JustArchiNET/ArchiSteamFarm · GitHub	github.com text/html	CONFIRM github.com/JustArchiNET/ArchiSteamFarm/security/advisories/GHSA-wxx4-66c2-vj2v
Fix GlobalConfig update via IPC removing IPCPassword by Abrynos · Pull Request #2379 · JustArchiNET/ArchiSteamFarm · GitHub	github.com text/html	MISC github.com/JustArchiNET/ArchiSteamFarm/pull/2379
Beware of unknown method which steal inventory through ASF IPC(on VPS) :: Archi's SC Farm	steamcommunity.com text/html	MISC steamcommunity.com/groups/archiasf/discussions/6/3057365873428498659/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Archisteamfarm Project	Archisteamfarm	All	All	All	All

cpe:2.3:a:archisteamfarm_project:archisteamfarm:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32794 : ArchiSteamFarm is a C# application with primary purpose of idling Steam cards from multiple accoun... twitter.com/i/web/status/1...	2021-07-26 18:57:12

← Previous ID

Next ID →

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)