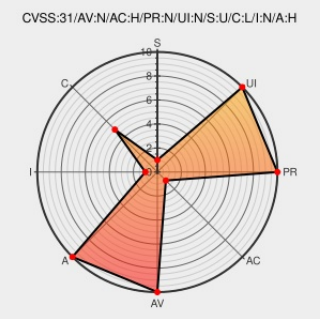
CVE-2021-32795

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

Last Modified on: 08/13/2021 06:23:00 PM UTC

CVE-2021-32795 - advisory for GHSA-5v34-4prm-9474

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



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. In versions prior to 4.3.1.0 a Denial of Service (aka DoS) vulnerability which allows attacker to remotely crash running ASF instance through sending a specifically-crafted Steam chat message exists. The user sending the message does not need to be authorized within the bot or ASF process. The attacker needs to know ASF's `CommandPrefix` in advance, but majority of ASF setups run with an unchanged default value. This attack does not allow attacker to gain any potentially-sensitive information, such as logins or passwords, does not allow to execute arbitrary commands and otherwise exploit the crash further. The issue is patched in ASF V4.3.1.0. The only workaround which guarantees complete protection is running all bots with `OnlineStatus` of `0` (Offline). In this setup, ASF is able to ignore even the specifically-crafted message without attempting to interpret it.

CVE-2021-32795 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **JustArchiNET** - **ArchiSteamFarm** version **>= 4.3.0.0, < 4.3.1.0**

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Avoid crash on commandPrefix message + hardening · JustArchiNET/ArchiSteamFarm@4cd581e · GitHub	github.com text/html	MISC github.com/JustArchiNET/ArchiSteamFarm/commit/4cd581ec041912cf19
Denial of Service via Steam chat · Advisory · JustArchiNET/ArchiSteamFarm · GitHub	github.com text/html	CONFIRM github.com/JustArchiNET/ArchiSteamFarm/security/advisor 9474
ASF Crash (raspbian) :: Archi's SC Farm	steamcommunity.com text/html	MISC steamcommunity.com/groups/archiasf/discussions/1/293574204

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-2021-32795 : ArchiSteamFarm is a C# application with primary purpose of idling Steam cards from multiple accoun… twitter.com/i/web/status/1…	2021-07-26 19:28:46

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report