Denial of Service via Steam chat (< 4.3.1.0)

Moderate **JustArchi** published **GHSA-5v34-4prm-9474** on Oct 14, 2020

Package

ArchiSteamFarm (GitHub)

Affected versions	Patched versions
Between ≥ 4.3.0.0 and < 4.3.1.0	≥ 4.3.1.0

Description

Impact

What kind of vulnerability is it? Who is impacted?

It's Denial of Service (aka DoS) vulnerability which allows attacker to remotely crash running ASF instance through sending a specifically-crafted Steam chat message. The user sending the message does not need to be authorized within the bot or ASF process. Other message channels (IPC and interactive console) are not affected. The attacker needs to know ASF's `CommandPrefix` in advance, which is impossible to achieve without prior brute-forcing attempts, but majority of ASF setups run with a sane, 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. It's only a crash of service (DoS), with no further implications, therefore of moderate severity.

Patches

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

The issue is patched in ASF V4.3.1.0 and future versions.

Workarounds

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

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.

It's possible to attempt to mitigate this problem by ensuring that users can't send the message to ASF bots through the Steam platform, therefore removing the attack vector, but due to the internals of Steam platform, it's impossible to achieve that entirely and therefore doesn't guarantee absolute protection.

References

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

The issue was originally reported at https://steamcommunity.com/groups/archiasf/discussions/1/2935742047969570844/

For more information

If you have any questions or comments about this advisory:

- Use our support channels.

Severity

Moderate 6.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	High

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

CVE ID

CVE-2021-32795

Weaknesses

No CWEs

Credits

JustArchi