



CVE-2023-40019

Published on: Not Yet Published

Last Modified on: 09/21/2023 06:04:00 PM UTC

CVE-2023-40019 - advisory for GHSA-gjj5-79p2-9g3q

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

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



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

FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.10.10, FreeSWITCH allows authorized users to cause a denial of service attack by sending re-INVITE with SDP containing duplicate

codec names. When a call in FreeSWITCH completes codec negotiation, the `codec_string` channel variable is set with the result of the negotiation. On a subsequent re-negotiation, if an SDP is offered that contains codecs with the same names but with different formats, there may be too many codec matches detected by FreeSWITCH leading to overflows of its internal arrays. By abusing this vulnerability, an attacker is able to corrupt stack of FreeSWITCH leading to an undefined behavior of the system or simply crash it. Version 1.10.10 contains a patch for this issue.

CVE-2023-40019 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **signalwire** - **freeswitch** version = < 1.10.10

CVSS3 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
Release FreeSWITCH v1.10.10 Release · signalwire/freeswitch	github.com	MISC

· GitHub

text/html

github.com/signalwire/freeswitch/releases/tag/v1.10.10

FreeSWITCH allows authorized users to cause a denial of service attack by sending re-INVITE with SDP containing duplicate codec names · Advisory · signalwire/freeswitch · GitHub

github.com

text/html

MISC

github.com/signalwire/freeswitch/security/advisories/GHSA-gjj5-79p2-9g3q

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	Freeswitch	Freeswitch	All	All	All	All
cpe:2.3:a:freeswitch:freeswitch:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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