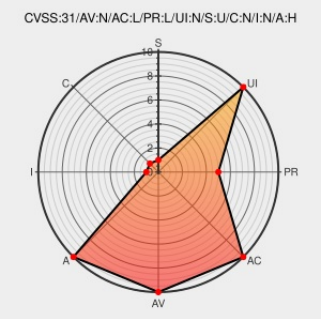
CVE-2023-40019

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



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

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→