contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

SignalWire FreeSwitch exploited

CVE-2026-116779 · on CISA's exploited list since 9 November 2026

Analysis Report

Teams running FreeSWITCH below version 1.11.3 must act by 12 November 2026 — two days from now. Check which version you run, then upgrade to 1.11.3.

PREPARED BY	NamiQ	DATE	10 November 2026
FACTS AS OF	10 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 12 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/signalwire-freeswitch-cve-2026-116779

The bottom line

> *Teams running FreeSWITCH below version 1.11.3 must act by 12 November 2026 — two days from now. Check which version you run, then upgrade to 1.11.3.*

At a glance

Fact	Detail
Product	SignalWire FreeSwitch (CVE-2026-116779)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 9 November 2026. Deadline for US federal agencies: 12 November 2026.
Chance of exploitation (EPSS)	0.02, the estimated chance in the next 30 days, as at 10 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	FreeSWITCH 1.11.3, released 28 August per the vendor's release notes on GitHub. The record lists all versions below 1.11.3 as affected.
Who looks first	Anyone running FreeSWITCH below 1.11.3 as a SIP server. The record says inbound chat is on in the stock internal and external profiles. The record says any authenticated profile account is sufficient to trigger the flaw.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run SignalWire FreeSWITCH anywhere in your environment?	Nothing to do for this CVE.	Check the version running (next question).
Is the version below 1.11.3?	No action needed for this CVE on that instance.	Treat this as urgent — read on.
Is inbound SIP chat or messaging enabled on that instance?	Exposure is reduced, but upgrade to 1.11.3 is still required.	Exposure is confirmed; upgrade to 1.11.3 immediately.
Can untrusted or external SIP peers authenticate to that instance?	Risk is lower; still upgrade to 1.11.3 before 12 November 2026.	High priority — upgrade now.

What it is

An authenticated SIP peer whose inbound MESSAGE is accepted can reach FreeSWITCH's API command layer, including operating-system commands running with the daemon's own privileges. The record also names configuration and credential disclosure and arbitrary call control as outcomes.

Why it matters

The flaw is in the inbound SIP MESSAGE handler, which is on by default in the stock internal and external profiles. The record says any authenticated profile account is sufficient to trigger it, and that stock directory users without password material can also remove that barrier. Our reading is that the effective bar for exploitation is very low in a standard deployment. Once reached, switch_api_execute() gives access to OS-level command sinks at the daemon's privilege level — the same as the telephony service itself.

What the vendor's advisory says

We read two pages on github.com. In short:

- The vendor's release notes call v1.11.3 an important release containing critical security fixes and stability improvements, and strongly encourage all users to upgrade as soon as possible.
- The release notes list two changes directly related to the MESSAGE handler: bounding the To-user split in mod_sofia, and adding an enable-chat-api-proto option to gate the API chat protocol in mod_sofia and mod_verto.
- The same release drops Debian 11 Bullseye support and fixes a timer syscall error in core. No other CVE identifiers are named in the release notes.

Things people will get wrong

- "Authentication is required, so the attack surface is small." The record says any authenticated profile account is sufficient and that stock directory users without password material can also remove that barrier, making the bar very low in a standard deployment.
- "The release notes don't name this CVE, so 1.11.3 may not fix it." The record lists versions below 1.11.3 as affected. The release notes describe bounding the To-user split in the inbound MESSAGE handler, which matches the described mechanism exactly.
- "This only affects internet-facing FreeSWITCH servers." The record does not restrict the flaw to internet-facing instances. Any SIP peer whose inbound MESSAGE is accepted can trigger it, including peers on internal networks.

The wording includes conditions the score may not show: it needs privileges; the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the FreeSWITCH version you run

- Check whether FreeSWITCH is installed on each server. The affected range is any version below 1.11.3.
- If installed via a package manager, check the package version. If built from source, check the version shown at startup.

Step 2: Check whether inbound SIP chat is enabled

- The record says inbound chat is enabled on the stock internal and external profiles. If your profiles are unmodified, assume it is on.
- Review your SIP profile configuration for any explicit disabling of MESSAGE handling or the api chat proto.

Step 3: Upgrade to FreeSWITCH 1.11.3

- The vendor's release notes call v1.11.3 a critical security release and strongly encourage all users to upgrade as soon as possible.
- CISA's deadline for this CVE is 12 November 2026. Plan and execute the upgrade now.
- After upgrading, the release notes note an enable-chat-api-proto option in mod_sofia and mod_verto to gate the API chat protocol.

Step 4: Confirm the installed version after upgrading

- Confirm the running version is 1.11.3 or later.
- Consider whether all SIP peers with authentication access are genuinely trusted, and tighten profile authentication where the record of trust is unclear.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We have been alerted to CVE-2026-116779, a code-injection vulnerability in SignalWire FreeSWITCH affecting all versions below 1.11.3. CISA has listed it with a remediation deadline of 12 November 2026. The flaw allows an authenticated SIP peer to reach operating-system command execution on the FreeSWITCH server. Please check whether FreeSWITCH is running in our environment, confirm the installed version, and advise whether any instance is below 1.11.3. If so, please confirm the upgrade plan and timeline to reach version 1.11.3. We would like written confirmation of the installed version and the fix status by 12 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected FreeSWITCH API command entries in the event or log output, particularly commands not issued by an operator, which may indicate switch_api_execute() was reached by an external peer.
- SIP MESSAGE traffic in logs with To: header user portions containing a plus sign, which the record identifies as the trigger path for the vulnerable API selector.

The weakness behind it

The record classes this as CWE-77 (Improper Neutralization of Special Elements used in a Command) and CWE-78 (Improper Neutralization of Special Elements used in an OS Command) and CWE-749 (Exposed Dangerous Method or Function).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so

Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	FreeSWITCH is typically a network-exposed SIP service; the flaw is triggered by an inbound SIP MESSAGE, making initial access likely via exploitation of a public-facing application.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The record states the flaw reaches switch_api_execute() including OS command sinks; successful exploitation would typically result in OS command or scripting interpreter execution.
Data from Local System (T1005): Copying data stored on the machine.	Collection: gathering data	The record and CISA description both name configuration and credential disclosure as outcomes, suggesting collection of local system data would likely follow exploitation.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *SignalWire FreeSwitch contains a code injection vulnerability that permits configuration and credential disclosure, arbitrary call control, and command execution.*

The CVE record, published by GitHub on 5 November 2026:

> *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 1.11.3, sofia_presence_handle_sip_i_message() split the To user of an inbound SIP MESSAGE on a plus sign and treated the left side as a chat protocol selector. Selecting the api chat proto reached switch_api_execute(), allowing a peer whose MESSAGE was accepted to run FreeSWITCH API commands, including operating-system command sinks, with the daemon's privileges. Inbound chat is enabled on the stock internal and external profiles, and any authenticated profile account is sufficient; stock directory ...*

Versions of signalwire freeswitch the record lists as affected:

- < 1.11.3

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-116779
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-116779
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not describe any workaround in pre-1.11.3 versions that disables the vulnerable API chat path without upgrading.
- The sources do not say whether hosted or cloud-managed FreeSWITCH deployments are patched by the provider or require customer action.
- The sources do not confirm any specific exploitation details beyond CISA's listing of this CVE.

- We have not tested this against any environment. Versions and scores are as the sources state them and as at 10 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-116779: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
5 November 2026	CVE record published by GitHub.
9 November 2026	CISA added it to its list of exploited vulnerabilities.
12 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
FreeSWITCH below 1.11.3 with inbound SIP reachable from the internet	High	Before 12 November 2026
FreeSWITCH below 1.11.3 on an internal network with untrusted or low-trust SIP peers	High	Before 12 November 2026
FreeSWITCH below 1.11.3 on an internal network with fully trusted SIP peers only	Medium	This week

FreeSWITCH 1.11.3 or later already in place	None	None for this CVE

Appendix 4. Definition of done

- Every SignalWire FreeSwitch you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-116779: https://www.cve.org/CVERecord?id=CVE-2026-116779
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: github.com/signalwire/freeswitch/security/advisories/GHSA-: https://github.com/signalwire/freeswitch/security/advisories/GHSA-mg63-h38w-8p9p
- Advisory or release notes read: github.com/signalwire/freeswitch/releases/tag/v1.11.3: https://github.com/signalwire/freeswitch/releases/tag/v1.11.3
- Reference in the CVE record: github.com: https://github.com/signalwire/freeswitch/pull/3135
- Reference in the CVE record: github.com: https://github.com/signalwire/freeswitch/commit/7015f6a73ab3d67fed5fbfc277ecfb88a74c2a86