GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

13 November 2026

Advisory 375: SignalWire FreeSWITCH Command Injection Vulnerability (CVE-2026-116779).

Release Date: 13th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-116779 is a critical command injection vulnerability (CWE-77) in FreeSWITCH, the open-source telephony platform maintained by SignalWire and used for VoIP, PBX and telecom services. It is rated CVSS 9.8. FreeSWITCH reads part of the recipient field of an inbound SIP MESSAGE as the name of a chat protocol. If that name is "api", the message is passed to the FreeSWITCH API and run as a command with the privileges of the FreeSWITCH server process.

What are the systems affected?

The vulnerability affects FreeSWITCH with inbound SIP chat enabled, which is the default:

- FreeSWITCH 1.11.2 and earlier
- VoIP and PBX systems, SIP trunks, contact centre platforms and telecom services built on FreeSWITCH
- Stock configurations that still contain the passwordless sample directory users, which let the attack succeed without credentials

Not affected / patched version:

- FreeSWITCH 1.11.3 or later
- Version 1.11.3 also includes the fixes for two other critical flaws, CVE-2026-116785 and CVE-2026-116790 (CVSS 9.1), which are not reported as exploited

What does this mean?

Successful exploitation may allow attackers to:

- Run commands on the server with the privileges of the FreeSWITCH process
- Read configuration files and SIP credentials
- Place, redirect or intercept calls, including fraudulent toll calls at the operator's expense
- Use the server as a foothold into the operator's network

Mitigation process

CERTVU recommends the following:

1. Upgrade to FreeSWITCH 1.11.3
Upgrade every FreeSWITCH instance to 1.11.3 or later, which blocks the "api" chat path by default and logs each blocked attempt with a 403 response. Some new security options in this release are turned off by default, so review the release notes and enable them.

2. Apply workarounds if you cannot upgrade yet
3. Restrict SIP exposure
4. Check for compromise

Report incidents to CERTVU at incident@cert.gov.vu.

Reference

1. https://github.com/signalwire/freeswitch/security/advisories/GHSA-mg63-h38w-8p9p
2. https://github.com/signalwire/freeswitch/releases/tag/v1.11.3
3. https://www.cve.org/CVERecord?id=CVE-2026-116779
4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-116779