

CVE-2019-19006

Sangoma FreePBX Improper Authentication Vulnerability

CISA KEV since Feb 3, 2026

Actively exploited

Sangoma FreePBX 115.0.16.26 and below, 14.0.13.11 and below, 13.0.197.13 and below have Incorrect Access Control.

EVRS 78 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.559 99.05th percentile · FIRST	CISA DEADLINE Feb 24, 2026 CISA federal deadline · Overdue by 8 months
---	---	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.559 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
freepbx	≥ 13.0.0.0 ≤ 13.0.197.13 ≥ 14.0.0.0 ≤ 14.0.13.11 ≥ 15.0.0.0 ≤ 15.0.16.26	after 13.0.197.13 · after 14.0.13.11 · after 15.0.16.26	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-85h5-chmw-697j	Additional guidance	community.freepbx.org/t/freepbx-security-vulnerability-sec-2019-001/62772
wiki.freepbx.org	wiki.freepbx.org/display/F0P/2019-11-20%2BRemote%2BAdmin%2BAuthentication%2BBypass	NVD	nvd.nist.gov/vuln/detail/CVE-2019-19006
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-8659
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-19006		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.