

CVE-2025-64328

Sangoma FreePBX OS Command Injection Vulnerability

CISA KEV since Feb 3, 2026

Actively exploited

Public exploit module (Metasploit)

FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. In versions 17.0.2.36 and above before 17.0.3, the filestore module within the Administrative interface is vulnerable to a post-authentication command injection by an authenticated known user via the testconnection -> check_ssh_connect() function. An attacker can leverage this vulnerability to obtain remote access to the system as an asterisk user. This issue is fixed in version 17.0.3.

EVRS 84/100 Urgent priority	CVSS V4.0 8.6 High · NVD	EPSS 0.846 99.71st 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	0.846 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.6	☐ 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
filestore	≥ 17.0.2.36 < 17.0.3	17.0.3	NVD

Sources

Vendor guidance	github.com/FreePBX/security-reporting/security/advisories/GHSA-vm9p-46mv-5xvw	NVD	nvd.nist.gov/vuln/detail/CVE-2025-64328
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-38232
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-64328		

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