POSTING DATE: 2025/12/23

[VULNERABILITY ALERT] Critical Security Vulnerability in Sangoma's FreePBX Phone Management System (CVE-2025-66039)

- Subject: [VULNERABILITY ALERT] Critical Security Vulnerability in Sangoma's FreePBX Phone Management System (CVE-2025-66039)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202512-00000008
  - FreePBX is an open-source IP phone management system by Sangoma, encompassing VOIP management, call forwarding, conferencing features, and more. Recently, FreePBX released a critical security advisory, stating that the FreePBX Endpoint Manager module contains an authentication bypass vulnerability (CVE-2025-66039, CVSS 4.x: 9.3). If the authentication type is set to “webserver”, the module allows for authentication bypass; if the value of the Authorization header is arbitrary, the session will be directed to the target user regardless of whether the credentials are valid.
- Affected Platforms:
  - FreePBX versions prior to 16.0.44 (exclusive)
  - FreePBX versions prior to 17.0.23 (exclusive)
- Recommended Actions:
  - Please update to the following versions: FreePBX version 16.0.44, FreePBX version 17.0.23
- Reference Material:
  - https://www.twcert.org.tw/tw/cp-169-10582-80c21-1.html

Computer and Communication Center
Network Systems Division, Respectfully

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251223_01

Last update: **2025/12/23 11:27**