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 RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICR DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPP 9108 Port-Vila, Vanuatu
Tél: (678) 33380

2 septembre 2025

Avis 97 : CVE-2025-57819 Vulnérabilité permettant de contourner l'authentification Sangoma FreePBX
Date de publication : 29 août 2025
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

CERT Vanuatu (CERTVU) et le service de Communication et de Transformation numérique (SCTN) publient la présente alerte.

Cette alerte concerne toutes les organisations et techniciens qui utilisent et gèrent ce produit.

Objet de l'alerte

CERTVU souhaite vous faire part de ce qui suit ;

- **CVE-2025-57819** est une vulnérabilité critique dans le module commercial « endpoint » des versions 15, 16 et 17 de FreePBX, causée par une insuffisance dans la désinfection des entrées fournies par l'utilisateur. Cette faille permet à des attaquants non authentifiés de contourner les contrôles d'accès administrateur, d'effectuer une injection SQL et, éventuellement, d'exécuter du code à distance.

Systèmes concernés

- **FreePBX 15** versions antérieures à la version 15.0.66.
- **FreePBX 16** versions antérieures à la version 16.0.89.
- **FreePBX 17** versions antérieures à la version 17.0.3.

Implication

Les attaquants peuvent exploiter cette faille par les manières suivantes :

- **Accès initial :** les attaquants exploitent les vulnérabilités liées aux entrées non sécurisées dans le module terminal pour contourner l'authentification et accéder à l'interface administrateur FreePBX.
- **Injection SQL :** Une fois dans le système, ils peuvent exécuter des requêtes SQL arbitraires pour manipuler la base de données.
- **Exécution de code à distance** : l'injection SQL est enchaînée pour permettre l'exécution de code à distance (RCE), potentiellement avec des privilèges de niveau root, donnant ainsi aux attaquants le contrôle total du système.

Mesures d'atténuation

CERTVU conseille au personnel informatique, aux administrateurs de système et aux techniciens d'appliquer immédiatement les mesures correctives suivantes :

- Immédiatement mettre à jour FreePBX vers l'une des versions corrigées suivantes :
  - **FreePBX 15** – 15.0.66
  - **FreePBX 16** – 16.0.89
  - **FreePBX 17** – 17.0.3
- Appliquez le contrôle de sécurité réseau en limitant l'accès administratif aux secteurs fiables à l'aide de règlements de pare-feu ou du module pare-feu FreePBX.
- Refuser tout accès externe jusqu'à ce que les systèmes soient corrigés.
- Surveillance constante des journaux du serveur Web afin de détecter tout trafic ou activité suspect dans votre réseau.

Références

1. https://www.cisa.gov/news-events/alerts/2025/08/29/cisa-adds-one-known-exploited-vulnerability-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-57819
3. https://nvd.nist.gov/vuln/detail/CVE-2025-57819