مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Zero-Day Vulnerability in FreePBX

Tracking #:432317654

Date-01-09-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The Sangoma FreePBX Security Team has issued an urgent warning regarding an actively exploited zero-day vulnerability affecting FreePBX systems that expose the Administrator Control Panel (ACP) to the public internet.

TECHNICAL DETAILS:

The Sangoma FreePBX Security Team has issued an urgent warning regarding an actively exploited zero-day vulnerability affecting FreePBX systems that expose the Administrator Control Panel (ACP) to the public internet. The flaw (CVE-2025-57819) has received a CVSS score of 10.0, indicating the highest severity level.

- CVE ID: **CVE-2025-57819**
- Severity: Critical (CVSS 10.0)
- Status: Actively Exploited
- Affected Products: FreePBX 15, 16, 17
- Impact: Remote Code Execution, Arbitrary Database Manipulation, Full System Compromise

Affected Versions:

- FreePBX 15: Versions prior to 15.0.66
- FreePBX 16: Versions prior to 16.0.89
- FreePBX 17: Versions prior to 17.0.3

Patched Versions:

- FreePBX 15: Versions 15.0.66
- FreePBX 16: Versions 16.0.89
- FreePBX 17: Versions 17.0.3

Indicators of Compromise (IOCs)

- File /etc/freepbx.conf recently modified or missing
- File /var/www/html/.clean.sh *should not exist on normal systems*
- POST requests to modular.php in web server logs *likely not legitimate traffic*
- Phone calls placed to extension 9998 in call logs and CDRs *are unusual - unless previously configured*
- Suspicious ampuser user in the ampusers database table *or other unknown users*

RECOMMENDATIONS:

- Upgrade to the latest patched versions.
- Search for the listed IoCs across systems and logs.
- Disconnect compromised systems from the network immediately if compromise is suspected.
- Restrict public access to the FreePBX Administrator Control Panel.
- Implement IP allowlisting and Access Control Lists (ACLs) for administrative interfaces.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h