Posted Date: 2025/09/04

[Vulnerability Alert] FreePBX has a high-risk security vulnerability (CVE-2025-57819), please confirm and patch as soon as possible

- Subject: [Vulnerability Alert] FreePBX has a high-risk security vulnerability (CVE-2025-57819), please confirm and patch as soon as possible
- Content:
  - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-200-202509-00000006
  - Researchers have discovered an Authentication Bypass vulnerability (CVE-2025-57819) in FreePBX, a web management interface tool for the Asterisk system. An unauthenticated remote attacker can directly access administrator functions, thereby controlling the database and executing arbitrary code. This vulnerability has already been exploited by hackers, so please confirm and patch it as soon as possible.
  - Note: Asterisk is an open-source private branch exchange (PBX) system software, including Voice over IP (VoIP) functionality. In addition to running on general computers, it can also run on embedded systems like OpenWRT.
- Affected Platforms:
  - FreePBX versions 15 to 15.0.66 (exclusive)
  - FreePBX versions 16 to 16.0.89 (exclusive)
  - FreePBX versions 17 to 17.0.3 (exclusive)
- Recommended Measures:
  - The official source has released a patch for the vulnerability; please refer to the official instructions at the following URL: https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2025-57819
  2. https://github.com/FreePBX/security-reporting/security/advisories/GHSA-m42g-xg4c-5f3h

---

Computer and Communications Center
Network Systems Group