Posted Date: 2025/11/12

[Vulnerability Alert] Samba has a high-risk security vulnerability (CVE-2025-10230), please confirm and patch as soon as possible

- Subject: [Vulnerability Alert] Samba has a high-risk security vulnerability (CVE-2025-10230), please confirm and patch as soon as possible
- Content:
  - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-200-202511-00000079
  - Researchers have discovered an Operating System Command Injection (OS Command Injection) vulnerability (CVE-2025-10230) in Samba. If a user deploys a Samba AD Domain Controller server and enables WINS protocol support, an unauthenticated remote attacker can inject arbitrary operating system commands and execute them on the Samba server.
- Affected Platforms:
  - Samba versions before 4.21.9 (exclusive)
  - Samba versions 4.22.0 up to 4.22.5 (exclusive)
  - Samba versions 4.23.0 up to 4.23.2 (exclusive)
- Recommended Measures:
  - The official source has released a fix update for the vulnerability; please refer to the official instructions for update at the following URL: https://www.samba.org/samba/history/security.html
- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2025-10230
  2. https://www.samba.org/samba/security/CVE-2025-10230.html
  3. https://www.samba.org/samba/history/security.html

Computer and Communications Center
Network Systems Group