مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Flaw in Samba AD DC

Tracking #:432317825

Date:16-10-2025

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 Samba Team has issued an urgent security advisory addressing two vulnerabilities affecting Samba Active Directory Domain Controllers.

TECHNICAL DETAILS:

The Samba Team has issued an urgent security advisory addressing two vulnerabilities affecting Samba Active Directory Domain Controllers (AD DCs).The first and most severe, CVE-2025-10230, is a critical command injection vulnerability with a maximum CVSS score of 10.0, allowing unauthenticated remote code execution (RCE).This issue arises when the WINS server feature is enabled with a configured “wins hook” parameter — a legacy mechanism for running external scripts on WINS name changes.

The second issue, CVE-2025-9640, is a medium-severity information disclosure flaw within the vfs_streams_xattr module that could allow authenticated users to read uninitialized memory fragments, potentially exposing sensitive data.

Administrators are strongly urged to apply the latest Samba patches immediately or disable affected features as an interim mitigation.

Critical Vulnerability Details:
1. CVE-2025-10230 – Command Injection via WINS Server Hook

- **Severity:** Critical
- **CVSS v3.1 Score:** 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
- **Affected Component:** WINS Server (Active Directory Domain Controller)
- **Affected Versions:** All versions since Samba 4.0
- **Fixed In:** Samba 4.23.2, 4.22.5, 4.21.9

RECOMMENDATIONS:

- Immediate Patch Deployment: Upgrade Samba installations to patched version or apply Short-Term Mitigation (If Patch Cannot Be Immediately Applied)

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://www.samba.org/samba/security/CVE-2025-10230.html