مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerabilities in Samba Suite

Tracking #:432319046

Date:01-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple critical vulnerabilities have been disclosed in the Samba suite affecting enterprise file and print-sharing infrastructure.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been disclosed in the Samba suite affecting enterprise file and print-sharing infrastructure. The most severe issue, CVE-2026-4480 (CVSS 10.0), enables unauthenticated remote code execution (RCE) via the Samba printing subsystem when misconfigured with the print command and %J substitution parameter.

Critical Vulnerability Details:

1. **CVE-2026-4480** (Critical RCE – CVSS 10.0)
   - Component Affected: Samba printing subsystem
   - Attack Vector: Remote, unauthenticated (in default guest-enabled configurations)
   - Root Cause:
     - CVE-2026-4480 Improper sanitization of %J substitution parameter in print command
     - Client-controlled print job description passed directly into shell execution context
     - Shell metacharacters are not escaped

2. **CVE-2026-4408** – Authentication Bypass / Privilege Escalation (CVSS 10.0)

Affected Software Versions:

Samba versions prior to:

- 4.22.10
- 4.23.8
- 4.24.3

Fixed Versions:

- 4.22.10 or later
- 4.23.8 or later
- 4.24.3 or later

RECOMMENDATIONS:

Immediate Actions:

- Upgrade all Samba deployments to patched versions.
- Apply vendor-provided security advisories immediately.

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-2026-4480.html
- https://www.samba.org/samba/security/CVE-2026-4408.html