

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Security Update Dell ThinOS 10

Tracking #:432318376

Date:10-02-2026

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 INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Dell has released security updates for ThinOS 10 to address multiple critical vulnerabilities affecting third-party components including OpenSSL, Samba, Google Chrome, and Amazon WorkSpace Client.

TECHNICAL DETAILS:

Dell has released security updates for ThinOS 10 to address multiple critical vulnerabilities affecting third-party components including OpenSSL, Samba, Google Chrome, and Amazon WorkSpace Client. These vulnerabilities could allow malicious actors to compromise affected thin client systems, potentially leading to unauthorized access, data exposure, denial of service, or remote code execution.

Affected Third-Party Components

Severity: CRITICAL

1. OpenSSL Vulnerabilities

- **CVE IDs:** CVE-2025-9232, CVE-2025-9231, CVE-2025-9230
- **Component:** OpenSSL cryptographic library

2. Samba Vulnerabilities

- **CVE IDs:** CVE-2025-10230, CVE-2025-9640
- **Component:** Samba file sharing service

3. Google Chrome Vulnerabilities

- **CVE IDs:** CVE-2025-13223, CVE-2025-13226, CVE-2025-13227, CVE-2025-13228, CVE-2025-13229, CVE-2025-13230, CVE-2025-12036
- **Component:** Google Chrome web browser (7 distinct vulnerabilities)

4. Amazon Workspace Client Vulnerabilities

- **CVE IDs:** CVE-2024-47601, CVE-2024-47602, CVE-2024-47603
- **Component:** Amazon Workspace Client

AFFECTED PRODUCTS & VERSIONS

Component	Vulnerable Versions	Remediated Version
ThinOS 10 Core	All versions < 2511_10.0380	2511_10.0380 or later
Google Chrome	Version 141.0.7390.76.279_T10 and earlier	143.0.7499.169.301_T10 or later
Amazon WorkSpace Client	Version 2025.0.4484.220_T10 and earlier	2025.1.5526.236_T10 or later

RECOMMENDATIONS:

- Upgrade Dell ThinOS 10 to fixed version or later.

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.dell.com/support/kbdoc/en-us/000415990/dsa-2026-056>