GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

11 September 2026

Advisory 300: Dell ThinOS 10 OS Command Injection and Access Control Vulnerabilities (CVE-2026-81467, CVE-2026-81046, and CVE-2026-81468).

Release Date: 10th September 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate Dell Wyse thin client devices running Dell ThinOS 10. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-81467, CVE-2026-81046, and CVE-2026-81468 are three critical vulnerabilities in Dell ThinOS 10, the purpose-built operating system running on Dell Wyse thin client devices, widely deployed by organizations and government agencies for virtual desktop infrastructure (VDI) and centrally-managed endpoint environments.
CVE-2026-81467 is an OS command injection flaw exploitable by an unauthenticated remote attacker.
CVE-2026-81046 is a protection mechanism failure (improper access control) also exploitable without authentication, allowing arbitrary code execution within the application context; and CVE-2026-81468 is a related OS command injection flaw requiring a high-privileged remote attacker. All three affect the same ThinOS 10 versions and share the same fixed release, so they are combined into this single advisory.

What are the systems affected?

The following version(s) are affected:

- Dell ThinOS 10, versions prior to 2605_10.2616 – (Affected)

Dell ThinOS 10, version 2605_10.2616 and later – (Not affected, patched)
A single update to ThinOS 10 version 2605_10.2616 resolves all three vulnerabilities. There is no separate workaround for any of the three, so upgrading is the only remediation.

What does this mean?

Typical attack flow:

1. **Reach the thin client remotely and inject OS commands or bypass access controls**
    - An unauthenticated remote attacker sends specially crafted input to a reachable Dell ThinOS 10 device, exploiting either the OS command injection flaw (CVE-2026-81467) or the access control failure (CVE-2026-81046) to execute arbitrary commands or code on the thin client, without any credentials.
2. **Execute further commands with elevated privileges**
    - Separately, an attacker who already holds high-privileged remote access to the device can exploit the related OS command injection flaw (CVE-2026-81468) to execute further arbitrary commands on the underlying system.

Attack vectors:

- A network-based attack against any Dell ThinOS 10 device reachable from an untrusted network; CVE-2026-81467 and CVE-2026-81046 require no authentication at all, while CVE-2026-81468 requires the attacker to already hold high-privileged remote access.
- No user interaction is required for any of the three

Successful exploitation may allow attackers to:

- Execute arbitrary commands or code on a Dell ThinOS 10 thin client device without authentication.
- Compromise the endpoint device used to access virtual desktop or centrally-managed environments, and potentially pivot into the wider network or VDI infrastructure it connects to.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Update Dell ThinOS 10 to version 2605_10.2616 or later on every managed thin client device, per Dell Security Advisory DSA-2026-389. A single update resolves all three vulnerabilities.

2. Restrict network access to thin client management interfaces

Report any suspected compromise of a Dell ThinOS 10 thin client device to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-81467
2. https://www.cve.org/CVERecord?id=CVE-2026-81046
3. https://www.cve.org/CVERecord?id=CVE-2026-81468
4. https://www.dell.com/support/kbdoc/en-us/000502746/dsa-2026-389-security-update-for-dell-thinos-10-for-multiple-vulnerabilities