

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Update-Dell Private Cloud VMware

Tracking #:432317646

Date:28-08-2025

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 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 Technologies has released a critical security update for Dell Private Cloud VMware to address multiple vulnerabilities affecting third-party components.

TECHNICAL DETAILS:

Dell Technologies has released a critical security update for Dell Private Cloud VMware to address multiple vulnerabilities in third-party components, primarily associated with SuSE Linux packages. These vulnerabilities could be exploited by a malicious actor to gain unauthorized access, escalate privileges, execute arbitrary code, or cause denial of service on affected systems.

Details:

The vulnerabilities exist due to security flaws in third-party components (SuSE packages) integrated with Dell Private Cloud VMware. These CVEs cover a wide range of issues including buffer overflows, race conditions, improper input validation, and privilege escalation flaws.

Notable Vulnerabilities Include:

- CVE-2025-1974
- CVE-2024-35221
- CVE-2024-58083
- CVE-2025-21635 to CVE-2025-22247

Affected Products:

- Dell Private Cloud VMware – Versions prior to 1.0.0.0

Remediation:

- Update to Version: 1.0.0.0 or later

RECOMMENDATIONS:

- Upgrade all Dell Private Cloud VMware installations to fixed version at the earliest.

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/000361580/dsa-2025-332-security-update-for-dell-private-cloud-vmware-vulnerabilities>