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

27 April 2026

Advisory 139: Microsoft Defender Insufficient Granularity of Access Control Vulnerability (CVE-2026-33825).

Release Date: 22nd April 2026
Impact: HIGH / 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 utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-33825 is a high-severity vulnerability (CVSS ~8.6) in VMware vCenter Server. The flaw is caused by improper input validation (CWE-20) within specific API endpoints exposed by vCenter.

What are the systems affected?

The vulnerability affects;

- **VMware vCenter Server** (multiple versions prior to the 2026 security updates)
- Both:
  - vCenter Server Appliance (VCSA)
  - Windows-based vCenter deployments (legacy)

Common environments at risk:

- Enterprise virtualization platforms
- Private cloud infrastructure
- Data centers managing VMware ESXi hosts

Because vCenter centrally manages virtual infrastructure, it is a high-value target.

What does this mean?

Exploitation is remote and network-based**,** requiring only HTTP access.

Typical attack flow:

1. **Target discovery**
   - Attackers scan for exposed vCenter instances (ports 443/5480).
2. **Crafted API request**
   - Malicious requests are sent to vulnerable vCenter API endpoints.
3. **Improper input validation triggered**
   - The server fails to sanitize or validate incoming data.
4. **Security control bypass**
   - The attacker manipulates request handling logic to gain unauthorized access.
5. **Remote code execution (in advanced exploitation)**
   - In certain scenarios, attackers may execute arbitrary commands on the vCenter server.

Successful exploitation of this vulnerability may allow attackers to:

- Gain unauthorized access to vCenter Server
- Execute arbitrary commands or code
- Control virtual machines and ESXi hosts
- Access sensitive infrastructure data
- Deploy malware or ransomware across virtual environments
- Disrupt services or shut down critical systems

Because vCenter controls the entire virtual infrastructure, compromise can lead to full data center takeover.

Mitigation process

CERTVU recommends the following:

1. Apply VMware Security Updates (Critical)

- Upgrade to patched versions of VMware vCenter Server released in 2026 advisories
- Ensure all vCenter instances are updated immediately

2. Restrict Management Interface Exposure

- Do not expose vCenter management interfaces directly to the internet
- Restrict access via:
  - VPN
  - Bastion hosts
  - Firewall allowlisting

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-33825
3. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33825

.