مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in ASUSTOR Data Master (ADM)

Tracking #:432318819

Date:21-04-2026



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical command injection vulnerability (CVE-2026-6644) has been identified in ASUSTOR's ADM operating system, specifically within its PPTP VPN client component.

## TECHNICAL DETAILS:

A high-severity command injection vulnerability (**CVE-2026-6644**, CVSS 9.4) has been identified in ASUSTOR's ADM operating system, specifically within its PPTP VPN client component. The flaw enables attackers—particularly those with administrative access—to execute arbitrary system commands, potentially resulting in full device compromise.
Given that ADM powers a wide range of ASUSTOR NAS devices, this vulnerability poses a significant risk to enterprise storage environments, SMB deployments, and individual users.

**Vulnerability Details**

- **CVE ID: CVE-2026-6644**
- **CVSS Score:** 9.4 (Critical)
- **Vulnerability Type:** Command Injection
- **Affected Component:** PPTP VPN Client (ADM interface)
- **Root Cause:** Improper input validation and lack of sanitization before shell execution

**Affected Versions**

- ADM 5.0 → Fixed in 5.1.3.RGL1 and later
- ADM 4.3 / 4.2 / 4.1 → Fixes in progress / not fully patched

**Attack Vector & Exploitation Flow**

- Exploitation requires authenticated administrative access.
- Malicious input is injected via the VPN client configuration interface.
- Unsanitized input is passed to system-level shell commands.
- Attackers can break out of restricted web management context.

**Impact**

- Remote Code Execution (RCE) on the NAS host
- Privilege escalation beyond intended administrative boundaries
- Full system takeover, including:
  - File system access (read/write/delete)
  - Data exfiltration or ransomware deployment
  - Persistence via backdoors or scheduled tasks

## RECOMMENDATIONS:

- Upgrade immediately: Apply ADM 5.1.3.RGL1 or later on all ADM 5.0 systems
- Disable PPTP VPN client if not strictly required
- Restrict administrative interface access to trusted IP ranges

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://nvd.nist.gov/vuln/detail/CVE-2026-6644