مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

# High-Severity Vulnerability in HP Client Management

Tracking #:432317917

Date:03-11-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HP has released a security update addressing a high-severity privilege escalation vulnerability (CVE-2025-11761) in its Client Management Script Library (CMSL) software.

## TECHNICAL DETAILS:

HP has released a security update addressing a high-severity privilege escalation vulnerability (CVE-2025-11761) in its Client Management Script Library (CMSL) software. The flaw, discovered during installation processes, could allow an attacker with local access to escalate privileges on affected systems.

Exploitation of this vulnerability could grant unauthorized elevated access, potentially enabling system modifications, installation of malicious software, or access to sensitive information. HP has issued a patched version (v1.8.5) and recommends that all users and IT administrators upgrade immediately via the PowerShell Gallery or the HP Client Management Solutions download page.

**Vulnerability Details**

- CVE ID: CVE-2025-11761
- CVSS v4.0 Score: 8.5 (High)
- HP Reference: HPSBHF04058 Rev. 1
- Affected Component
  - Software: HP Client Management Script Library (CMSL)
  - Impacted Versions: Prior to v1.8.5
- Fixed Version: HP Client Management Script Library 1.8.5 or later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update HP CMSL across all endpoints running affected versions.

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://support.hp.com/us-en/document/ish_13187651-13187675-16/hpsbhf04058