مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

HP ThinPro Security Update

Tracking #:432318440

Date:03-02-2026

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed HP has released HP ThinPro 8.1 SP9 to address multiple critical, high, and medium severity security vulnerabilities affecting earlier versions of HP ThinPro.

TECHNICAL DETAILS:

HP has released HP ThinPro 8.1 SP9 to address multiple critical, high, and medium severity security vulnerabilities affecting earlier versions of HP ThinPro. These vulnerabilities span core system components, multimedia frameworks, cryptographic libraries, networking services, and the Linux kernel. Several of the identified flaws carry Critical CVSS scores (9.8–10.0) and may allow unauthenticated remote attackers to execute arbitrary code, escalate privileges, compromise confidentiality and integrity, or cause denial-of-service conditions.

Vulnerability Details

- Severity: Critical
- Release Date: February 2, 2026
- Product: HP ThinPro (Cloud Client Software)
- Affected Versions: All HP ThinPro versions prior to 8.1 SP9
- Fixed Version: HP ThinPro version 8.1 SP9

Critical Vulnerabilities Overview

The following vulnerabilities are classified as **Critical** due to their exploitability, impact, and attack surface.

1. Samba – Remote Code Execution
   - CVE ID: CVE-2025-10230
   - CVSS Score: 10.0 (Critical)

2. FFmpeg – Remote Code Execution
   - CVE ID: CVE-2024-35368
   - CVSS Score: 9.8 (Critical)

3. FFmpeg – Remote Code Execution
   - CVE ID: CVE-2024-35366
   - CVSS Score: 9.1 (Critical)

4. FFmpeg – Remote Code Execution
   - CVE ID: CVE-2024-35367
   - CVSS Score: 9.1 (Critical)

5. WebKitGTK – Remote Code Execution
   - CVE ID: CVE-2025-43343
   - CVSS Score: 9.8 (Critical)

6. WebKitGTK – Remote Code Execution
   - CVE ID: CVE-2025-43342
   - CVSS Score: 9.8 (Critical)

RECOMMENDATIONS:

Immediate Actions (High Priority)

- Upgrade all HP ThinPro devices to fixed version immediately
- Prioritize internet-facing and high-privilege systems
- Validate successful installation across endpoints

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_13919531-13919557-16/hpsbhf04084