

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Local Privilege Escalation Vulnerability in HP Support Assistant

Tracking #:432317352

Date:09-06-2025

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 HP has disclosed a high-severity vulnerability (CVE-2025-43026) affecting HP Support Assistant, a tool widely used on HP PCs for system updates, diagnostics, and support access.

TECHNICAL DETAILS:

HP has disclosed a high-severity vulnerability (CVE-2025-43026) affecting HP Support Assistant, a tool widely used on HP PCs for system updates, diagnostics, and support access. This flaw, present in versions prior to 9.44.18.0, may allow local attackers to escalate privileges by exploiting an arbitrary file write condition. Exploiting this vulnerability could grant elevated access to unauthorized users and potentially lead to denial-of-service (DoS) conditions or compromise of system integrity.

Vulnerability Details:

- CVE ID-CVE-2025-43026
- CVSS v4.0 Base Score 7.1 (High)
- Impact-Escalation of Privileges, Denial of Service
- Exploit Technique-Arbitrary file write
- Affected Component-HP Support Assistant
- Fixed Version-9.45.11.0

RECOMMENDATIONS:

- Update HP Support Assistant to fixed version.

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_12617979-12618008-16/hpsbgn04022