مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Critical Vulnerabilities in HP Device Manager

Tracking #:432318552

Date:10-03-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed HP Device Manager (HPDM) contain multiple security vulnerabilities that could allow attackers to compromise affected systems.

TECHNICAL DETAILS:

HP Device Manager (HPDM) versions prior to 5.0.16 contain multiple security vulnerabilities that could allow attackers to compromise affected systems. These vulnerabilities originate from several integrated components and third-party libraries used within the platform.

Successful exploitation could enable remote code execution, privilege escalation, denial of service (DoS), and sensitive information disclosure. Some of the identified vulnerabilities have CVSS scores up to 9.8 (Critical), indicating a high likelihood of exploitation in vulnerable environments.

Key Vulnerabilities Identified
Critical Vulnerabilities

- **CVE-2023-38545** – (CVSS 9.8)
  - Component: cURL
- **CVE-2025-55754** – (CVSS 9.6)
  - Component: Apache Tomcat
- **CVE-2025-23048** – (CVSS 9.1)
  - Component: Apache HTTP Server

Product Affected
HP Device Manager

- Affected Versions: All versions prior to 5.0.16
- Patched Version: HP Device Manager 5.0.16

RECOMMENDATIONS:

Immediate Mitigation

- Upgrade HP Device Manager to fixed version or later.

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/nz-en/document/ish_14442335-14442364-16/hpsbhf04092