مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in HP LaserJet Printers

Tracking #:432316876

Date:17-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in certain HP LaserJet printers that could be exploited to execute malicious code and potentially gain control of the affected devices.

TECHNICAL DETAILS:

Vulnerabilities Details:

- CVE-2025-26506: CVSS Score: 9.2 (Critical)
- CVE-2025-26508: CVSS Score: 8.3 (High)
- CVE-2025-26507: CVSS Score: 6.3 (Medium)
- Multiple vulnerabilities exist in certain HP LaserJet Pro, HP LaserJet Enterprise, and HP LaserJet Managed Printers. These vulnerabilities could allow for Remote Code Execution (RCE) and Elevation of Privilege (EoP) when processing a PostScript print job.
- Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code on the affected device. This could potentially compromise sensitive information and grant unauthorized access to the network.

Note: Refer to HP Security Bulletins for affected products, fixed firmware versions, and more details.

RECOMMENDATIONS:

- **Update Firmware:** Download and install the latest firmware updates provided by HP for the affected printer models.
- **Restrict Network Access:** Limit access to the printers from untrusted networks and implement network segmentation where applicable.
- **Disable Unused Services:** Disable unnecessary printing protocols and services to reduce exposure.
- **Monitor for Unusual Activity:** Regularly check printer logs and network activity for any signs of suspicious behavior.

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_11953771-11953793-16/hpsbpi04007