مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Local Privilege Escalation Vulnerability in Epson Printer Drivers

Tracking #:432317144

Date:29-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in EPSON printer drivers for Windows operating systems. This vulnerability could be exploited to execute malicious code with SYSTEM-level privileges on affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-42598**
- A local privilege escalation vulnerability exists in Epson printer drivers installed on non-English versions of Microsoft Windows operating systems. This vulnerability allows an attacker with local access to overwrite specific DLL files managed by the driver with arbitrary code, potentially gaining SYSTEM-level privileges.
- Exploitation of this vulnerability could result in:
  - Unauthorized privilege escalation on affected systems.
  - Arbitrary code execution with all account privileges.

Affected Products:

The vulnerability impacts Epson Printer Drivers installed on the following operating systems:

- **Windows OS:** Windows XP/XP Professional x64 Edition, Vista/Vista x64, 7/7 x64, 8/8 x64, 8.1/8.1 x64, 10/10 x64, 11 x64.
- **Windows Server:** Server 2003, 2008/2008 R2, 2016, 2019, 2022, and Server 2025.

RECOMMENDATIONS:

- **Apply the Security Patch:** Install the patch provided by Epson. Use the Epson Software Updater or download the patch from Epson's official website.
- Regularly update all device drivers and firmware.
- Implement network segmentation for printers and IoT devices.
- Monitor endpoint logs for suspicious activity, particularly in directories associated with Epson drivers.

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://www.epson.co.uk/en_GB/faq/KA-01993/contents?loc=en-us