مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Flaw in SATO Industrial Label Printers
Tracking #:432317576
Date:08-08-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two critical security flaws in SATO Corporation's widely deployed industrial label printers that could allow remote attackers to execute arbitrary commands or gain root-level access to affected devices.

TECHNICAL DETAILS:

Vulnerability Details:
- **CVE-2025-22470 – Unrestricted Upload of Dangerous File Type**
- **Severity:** Critical (CVSS v3.1 Score: 9.8)
- This flaw enables attackers to upload and execute arbitrary Lua scripts on the printer with root privileges, potentially leading to full device compromise, data manipulation, or use of the printer as a pivot point for further attacks

- **CVE-2025-22469 – OS Command Injection**
- **Severity:** High (CVSS v3.1 Score: 7.3)
- This vulnerability allows remote attackers to execute arbitrary operating system commands using a specific non-administrative user account. Exploitation could lead to unauthorized control over printer functions and potential lateral movement within the network

Affected Products and Versions:
- CL4/6NX Plus – Firmware versions prior to 1.15.5-r1
- CL4/6NX-J Plus – Firmware versions prior to 1.15.5-r1

Fixed Version
- Firmware Version: 1.15.5-r1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates released by the Vendor.

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://nvd.nist.gov/vuln/detail/CVE-2025-22469
- https://nvd.nist.gov/vuln/detail/CVE-2025-22470