Security Advisory – 1XX Series

Summary

A stored Cross-Site Scripting (XSS) vulnerability exists in certain 1xxx series NVR devices due to insufficient sanitization of user-supplied input in specific functional modules. Attackers can inject malicious scripts, which are then persistently stored on the device backend. When administrators or users access affected pages, the stored scripts are executed in their browsers, leading to potential session hijacking, unauthorized actions, or data theft.

Vulnerability Score

The vulnerability has been assessed using the CVSS v4.0 standard.

- **Score:** 6.8 (Medium)
- **Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Affected Products

Model	Affected Version	Fixed Version
CP-UNR- 108F1	V4.001.00AT009.0.R	CP-UNR-Axxx-Mars_PN_15_Q_00_V1.00.14.01.T.260326
CP-UNR- 104F1	V4.001.00AT009.0.R	CP-UNR-Axxx-Mars_PN_15_Q_00_V1.00.14.01.T.260326

Fix Software Download

Users are strongly advised to upgrade to the latest firmware version.

Fixed Version:

CP-UNR-Axxx-Mars_PN_15_Q_00_V1.00.14.01.T.260326

- **Revision History**

Version	Description	Date
V1.0	Initial public release	28-March-2026

Source: CPPLUS would like to thank Mr. Jithin Nambiar J, a security researcher, for reporting this vulnerability.

For firmware access and upgrade instructions, please contact support.

Support Contact

- **Phone:** +91-8800952952
- **Email:** support@cpplusworld.com