NATIONAL CSIRT-CY

CVE-2025-5124 **25/05/2025**

Sony Network Cameras - Default Credential Vulnerability Enables Unauthorized Access

Executive Summary

The SONY Network Camera SNC series (including models SNC-M1, SNC-M3, SNC-RZ25N, SNC-RZ30N, SNC-DS10, SNC-CS3N, SNC-RX570N, and others) is affected by a critical security vulnerability caused by the use of hard-coded default credentials (admin:admin) in the administrative interface. Attackers can exploit this flaw to gain full administrative control over the device by leveraging the unmodified default credentials to access privileged management interfaces.

Analysis

Firmware versions are affected if they either do not require a credential change upon first login or continue to allow the use of default credentials (e.g., admin/admin). Although the specific impacted versions may differ by model, all confirmed vulnerable cases were found running firmware earlier than version 1.30.

The administrative interface is accessible through multiple ports (e.g., 8000, 8080, 1025, 3333, etc.), depending on the device's configuration, and is reachable via different web paths that vary across device subseries. Examples of vulnerable paths include:

- /adm/file.cgi?next_file=setting.htm
- /en/l4/advance.html
- /home/l4/admin_top2.html
- other device-specific administrative URLs

Exploiting the vulnerability successfully enables attackers to:

1. Change administrative passwords, granting them continued unauthorized access.
2. Reconfigure network settings (such as DNS or IP parameters), which can be used to launch man-in-the-middle attacks or pivot within the network.
3. Access sensitive device data or firmware, potentially supporting further reverse engineering efforts.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/1392.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-5124

Affected Products

The following products with firmware versions prior to 1.30:

- SONY Network Camera SNC-M1
- SONY Network Camera SNC-M3
- SONY Network Camera SNC-RZ25N
- SONY Network Camera SNC-RZ30N

- SONY Network Camera SNC-DS10
- SONY Network Camera SNC-CS3N
- SONY Network Camera SNC-RX570N
- Other SNC series devices using default credentials

Solutions

- **Update firmware to a version later than 1.30**
- **Change default credentials**

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.