CVE-2026-34005

CVE-2026-34005: OS Command Injection via Hostname Configuration in Xiongmai DVR/NVR (Sofia)

View the Project on GitHub uky007/CVE-2026-34005

CVE-2026-34005: OS Command Injection via Hostname Configuration in Xiongmai DVR/NVR (Sofia)

Summary

An OS command injection vulnerability exists in the hostname configuration handling path of the **Sofia** binary used in certain Xiongmai DVR/NVR devices running firmware **V4.03.R11**. In the affected code path, user-controlled hostname input is incorporated into a shell command and then executed via `system()` without sufficient sanitization.

Based on static analysis, reverse engineering, and instruction-level emulation, this issue may allow an **authenticated** attacker to execute arbitrary OS commands with **root privileges** through the DVRIP configuration interface.

This write-up is limited to the two confirmed models listed below. It does **not** claim broader product coverage beyond those models and firmware builds.

- **CVE ID:** CVE-2026-34005
- **CWE:** CWE-78 (OS Command Injection)
- **Authentication:** DVRIP authentication required
- **Affected protocol / service:** DVRIP (`TCP/34567`)

Affected Products

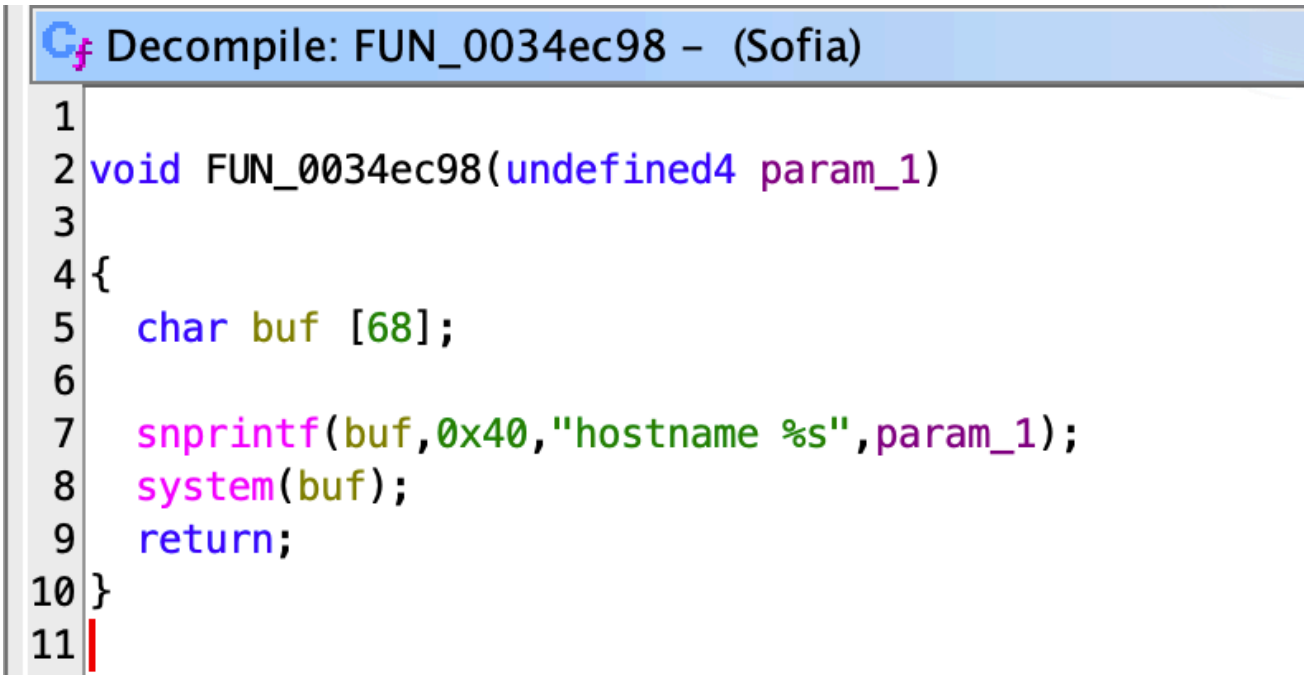
The following models and builds were confirmed during firmware analysis:

Device Type	Model	Firmware	Build Date
DVR	AHB7008T-MH-V2	V4.03.R11	2019-09-09
NVR	NBD7024H-P	V4.03.R11	2019-05-29

Technical Details

The affected functionality is the **hostname configuration handler** inside the Sofia binary. The vulnerable path is reached through the DVRIP protocol by setting the `HostName` field under the `NetWork.NetCommon` configuration category.

The vulnerable pattern is straightforward:



In other words, attacker-controlled input is formatted into a shell command and passed directly to `system()` without validation, escaping, or other defensive handling.

Representative Evidence

During reverse engineering, the following behavior was observed:

- a format string equivalent to `"hostname %s"`
- construction of a command buffer via `snprintf`
- immediate execution of that buffer via `system()`
- no filtering or escaping between input handling and command execution

The same vulnerable code pattern was confirmed in both analyzed firmware lines.

Verification Basis

This finding is based on **firmware analysis only**. No live devices were accessed during this research.

Validation methods used:

- **Disassembly** to identify the `snprintf(... "hostname %s" ...) -> system()` pattern
- **Decompiler review** to confirm the missing validation in the hostname path
- **Instruction-level emulation** to confirm that crafted input reaches `system()` unchanged
- **QEMU user-mode execution** to validate binary viability in an emulated ARM environment

Impact

If a valid DVRIP-authenticated actor can reach the hostname configuration path, shell metacharacters in the hostname value may be interpreted by the shell, leading to arbitrary command execution with root privileges.

This public note intentionally avoids including weaponized exploitation payloads.

Relationship to Previously Disclosed Issues

This issue was reviewed against previously disclosed Xiongmai-related CVEs and treated as distinct based on input path, protocol, and vulnerability class.

Examples of compared issues included:

- CVE-2022-45045 — DVRIP OPMachine/DebugShell path, different handler
- CVE-2024-3765 — authentication bypass, different vulnerability class
- CVE-2021-43517 — macGuarder service (port 9530), different service
- CVE-2018-10088 — HTTP uc-httpd buffer overflow, different protocol and bug class
- CVE-2022-45460 — HTTP buffer overflow, different protocol and bug class
- CVE-2017-7577 — HTTP path traversal, different protocol and bug class
- CVE-2022-26259 — RTSP overflow, different protocol and bug class

Mitigation Guidance

The most appropriate remediation is to eliminate shell invocation from this code path.

Recommended fixes:

1. Replace `system()` with a non-shell API such as `sethostname()`.
2. Validate hostname input against a strict allowlist.

3. Reject or escape shell metacharacters as defense in depth.

Disclosure Timeline

Date	Event
2026-03-20	Attempted vendor contact to XMSRC@xiongmaitech.com
2026-03-20	Vendor contact failed with `554 5.7.1 Relay access denied`
2026-03-20	CVE request submitted to MITRE CNA-LR
2026-03-25	CVE-2026-34005 assigned by MITRE
2026-03-27	Public technical note published

Credit

Discovered by **uky**.
