No: W-43/11/2021-IPHW

Government of India

Ministry of Electronics and Information Technology
IPHW Division
****

Electronics Niketan
6CGO Complex,
Lodhi Road, New Delhi-110003
Dated: 26.11.2025

CIRCULAR

Subject: Process for updating software components for ER- Certified IP Cameras-reg

Objective:

To ensure that any component used in ER-certified IP camera firmware including third-party libraries, system utilities, the Linux kernel, bootloaders, or other firmware modules changed due to End-of-Life (EoL) or feature changes, vulnerability fixes or any other reasons are identified, replaced and informed to regulatory authorities.

2. Continuous Monitoring

OEM must maintain a Software and Hardware bill of material Inventory Register, tracking:

(i) Component name and version

(ii) Role of component in the firmware

(iii) Last update date

(iv) EoL status from upstream project

(v) Known CVEs

(vi) Compliance relevance in respect of ER

3. Trigger for Impact Analysis

Initiate the Impact Analysis if any of the following (including but not limited to) occurs:

(i) Emergency fixes due to vulnerability exposure or glitches.

(ii) Voluntary update in software due to any reason

(iii) Change in code after public declaration of EoL by the component maintainers from genuine source.

(iv) Change of Security Critical components.

(v) Other changes like lens or any other non-security critical component.

4. Type of Changes:

(i) Major changes: These types of changes have impact on security of the IP Camera.

(ii)Minor changes: These types of changes are cosmetic types and have no impact on security of the IP Cameras. The list of minor changes is as under:

(i) Text changes (menu labels, spelling corrections, translation updates).

(ii) Minor color/theme adjustments in web interface or OSD menus.

(iii) Icon replacements without functional change.

(iv) Changes in log messages format.

(v) Including additional text

(vi) Changing default values for brightness, volume, display.

(vii) Correcting grammar/translation issues.

(viii) Font updates for multi-language display.

(ix) Boot-up splash screen/logo change.

(x) Audio tones/beeps adjustment.

(xi) Rearranging menu structure without removing/adding core features.

(xii) Adding tooltips or inline descriptions in UI.

All other changes not explicitly mentioned under minor changes are considered as major changes.

5. The OEM must implement necessary remediation (offline/online

Firmware updates) as given below for change in software components:

(i) There should not be any EoL libraries in the firmware. The manufacture must initiate action in advance as per the EOL notice from Original Library source and based on major/minor changes, action shall be initiated for updating the firmware after such changes are placed on records/ approved (as applicable) by BIS. The devices with EoL libraries and unable to be updated even after expiry of six months of EoL date, shall be considered non complaint and action will be initiated as per the BIS Act, 2016.

(ii) For emergency fixes, due to vulnerability disclosure/discovery, the patching may be done immediately. However, the impact analysis report shall be submitted to BIS within 10 working days for placing the same on record. Subsequently, the verification report based on appropriate testing as received from the BIS recognized laboratory shall be submitted to BIS for approval. Feature addition shall not be treated as emergency fixture.

(iii) For major feature addition and other changes, the verification report from lab shall be submitted to BIS for approval, subsequent to which the updates shall be rolled out.

(iv) For minor changes, the OEM shall submit the Impact analyst report and revised hash code to BIS for placing on records, subsequent to which the updates shall be rolled out.

(v)

6. Prepare Impact Analysis Report

This report is mandatory for BIS submission and should include:

(i) General Info

a. Model name and ER certification number with SoC detail

b. Firmware version hash before and after the change

c. Description of the components being changed and its function

(ii) Risk Assessment

(i) Is the component security-critical? (Y/N)

(ii) Are there known vulnerabilities? (List CVEs)

(iii) Exposure vector (e.g., LAN, cloud, UI)

(iv) Security feature affected (boot, encryption, login)

(iii) Mitigation / Replacement Plan

(i) New component or version integrated

(ii) Functional and regression test results

(iii) Secure boot/signing changes (if any)

(iv) Static code scan results

(v) New firmware hash (SHA-256)

7. Upload to BIS Portal

OEM must:

(i) Log into BIS Portal

(ii) Select certified model

(iii) Declare change as Major/Minor

(iv) Upload:

a. EoL Impact Analysis Report (PDF)/ Verification Report from Lab (as applicable as per provisions at Sl No 5)

b. Static Source Code Scan Report

c. Firmware hash

d. Secure boot proof/logs (if applicable)

8. Surveillance Audit Review

During the regular surveillance, MeitY may:

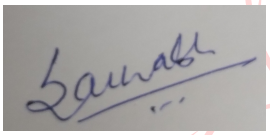
(i) Request firmware binary for hash match

(ii) Verify secure boot is enabled and working

(iii) Check kernel or bootloader version

(iv) Request updated source code scan report

(v) Review mitigation of known CVEs.



Digitally signed by Saurabh Ranjan
DN: c=IN, o=Ministry of Electronics and Information Technology, ou=MEITY, 2.5.4.20=d0388b5e02ae1ee7568e4656def5ad5b92699a3387dc00256b431ee8b8c5c72a, postalCode=110003, st=Delhi, serialNumber=64ba24570dd2e2b8319c2aa44672d3da26730e9794f0a6b0462ffb93863d6dee, cn=Saurabh Ranjan
Date: 2025.11.26 10:33:45 +05'30'

(Saurabh Ranjan)
Scientist 'D'
Tel:011-24301229
Email: Saurabh.r@gov.in

To,

i. Industry Associations
ii. Bureau of Indian Standards
iii. Website of MeitY
iv. STQC