CRA Rapid Reporter

Reporting Preparation & Evidence Pack

DEMONSTRATION OUTPUT — NOT FOR SUBMISSION

Case: Actively exploited vulnerability in AcmeVision Smart Camera

Case ID	DEMO-SMART-CAMERA-2026
Report type	Actively exploited vulnerability
Status	REVIEW
Completeness	100% (13/13)
Generated	2026-07-11 22:51 UTC

Manufacturer and product

Manufacturer: AcmeVision Devices Ltd. (fictional)

Manufacturer country: Singapore

EU main establishment / coordinator country: Germany

Reporting contact: Maya Chen psirt@example.invalid

Product: AcmeVision HomeCam X2

Model / identifier: AV-HCX2

Product version: 4.3.1

Affected versions: 4.0.0–4.3.1

Known Member States: Germany, France, Netherlands, Spain

Timeline and calculated preparation deadlines

Discovered: 2026-07-10T06:30+00:00

Manufacturer awareness: 2026-07-10T08:00+00:00

24-hour early warning due: 2026-07-11T08:00Z

72-hour notification due: 2026-07-13T08:00Z

Final report due: 2026-07-25T04:00Z

Final report basis: 14 days after a corrective or mitigating measure became available

Assessment

Summary: A command-injection vulnerability in the remote diagnostics endpoint is reported as actively exploited against internet-exposed devices.

Nature / exploit / incident: Unauthenticated crafted requests can reach a legacy diagnostics handler. Available telemetry indicates automated exploitation from multiple source networks.

Initial assessment: Exposure is limited to devices with remote diagnostics enabled and directly reachable from the public internet.

Severity: critical

Severity and impact: Successful exploitation may allow arbitrary command execution, unauthorised access to camera feeds and configuration changes.

Affected data or functions: Video stream confidentiality, device configuration integrity and service availability.

Suspected malicious acts: yes

Malicious actor information: No reliable attribution available. Activity appears opportunistic and automated.

Likely threat / root cause: Legacy diagnostics handler did not validate shell metacharacters before invoking a system utility.

Malicious code possible: Yes

Corrective and mitigating measures

Measures taken: Disabled cloud relay access to the diagnostics endpoint and deployed server-side blocking rules.

User measures: Disable remote diagnostics, restrict device network exposure and apply firmware 4.3.2 when available.

Security update / corrective measure: Firmware 4.3.2 removes the legacy handler and replaces the utility call with a parameter-safe implementation.

Applied and ongoing actions: Customer notification draft, affected fleet analysis and retrospective log review.

Information handling

Sensitivity: sensitive

Confidentiality notes: Exploit details should be handled under coordinated disclosure until the update is broadly available.

Review record

Reviewer: Alex Morgan

Role: Product Security Lead

Decision: review

Notes: Demonstration data only. Confirm affected Member States and corrective-measure availability time.

Approved at: Not provided

Completeness review

No required preparation fields are missing under the current internal checklist.

Evidence index

No evidence files attached.