Anviz CX7 Firmware Use of Hard-coded Cryptographic Key

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-32324
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 20:16:33 UTC
Updated	2026-04-17 20:16:33 UTC
Description	Anviz CX7 Firmware is vulnerable because the application embeds reusable certificate/key material, enabling decryption o

Risk And Classification

Primary CVSS: v3.1 7.7 HIGH from ics-cert@hq.dhs.gov

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Problem Types: CWE-321 | CWE-321 CWE-321 Use of Hard-coded Cryptographic Key

Version	Source	Type	Score	Severity	Vector
3.1	ics-cert@hq.dhs.gov	Secondary	7.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	7.7	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Anviz	Anviz CX7 Firmware	affected All versions	Not specified

References

Reference	Source	Link	Tags
www.cisa.gov/news-events/ics-advisories/icsa-26-106-03	ics-cert@hq.dhs.gov	www.cisa.gov	
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-10...	ics-cert@hq.dhs.gov	github.com	
www.anviz.com/contact-us.html	ics-cert@hq.dhs.gov	www.anviz.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Workarounds

CNA: Anviz did not respond to CISA's attempts to coordinate these vulnerabilities. Users should contact Anviz for more information at https://www.anviz.com/contact-us.html.

There are currently no legacy QID mappings associated with this CVE.