Anviz Products Download of Code Without Integrity Check

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

Summary

CVE	CVE-2026-40066
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 20:16:35 UTC
Updated	2026-04-17 20:16:35 UTC
Description	Anviz CX2 Lite and CX7 are vulnerable to unverified update packages that can be uploaded. The device unpacks and exec

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from ics-cert@hq.dhs.gov

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

Problem Types: CWE-494 | CWE-494 CWE-494

Version	Source	Type	Score	Severity	Vector
3.1	ics-cert@hq.dhs.gov	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Anviz	Anviz CX7 Firmware	affected All versions	Not specified
CNA	Anviz	Anviz CX2 Lite 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.