



Anviz CrossChex Standard Improper Verification of Source of a Communication Channel

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-40434
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 20:16:36 UTC
Updated	2026-04-17 20:16:36 UTC
Description	Anviz CrossChex Standard lacks source verification in the client/server channel, enabling TCP packet injection by an attack

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from ics-cert@hq.dhs.gov

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

Problem Types: CWE-940 | CWE-940 CWE-940

Version	Source	Type	Score	Severity	Vector
3.1	ics-cert@hq.dhs.gov	Secondary	8.1	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	8.1	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Anviz	Anviz CrossChex Standard	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.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report