



# America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

## ICS ADVISORY

# Anviz Multiple Products

**Release Date:** April 16, 2026

**Alert Code:** ICSA-26-106-03

**RELATED TOPICS:** [INDUSTRIAL CONTROL SYSTEM VULNERABILITIES](#) </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, [INDUSTRIAL CONTROL SYSTEMS](#) </topics/industrial-control-systems>

**View CSAF** <[https://github.com/cisagov/csaf/blob/develop/csaf\\_files/ot/white/2026/icsa-26-106-03.json](https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2026/icsa-26-106-03.json)>

## Summary

**Successful exploitation of these vulnerabilities could allow attackers to conduct reconnaissance, capture or decrypt sensitive data, alter device configurations, gain unauthorized administrative or root-level access, execute arbitrary code, compromise credentials or communications, and ultimately obtain full control over affected devices.**

The following versions of Anviz Multiple Products are affected:

- CX2 Lite Firmware vers:all/\* (CVE-2026-32648, CVE-2026-40461, CVE-2026-35682, CVE-2026-35546, CVE-2026-40066, CVE-2026-33569)
- CX7 Firmware vers:all/\* (CVE-2026-33093, CVE-2026-35061, CVE-2026-32648, CVE-2026-40461, CVE-2026-35546, CVE-2026-40066, CVE-2026-32324, CVE-2026-31927, CVE-2026-33569)
- CrossChex Standard vers:all/\* (CVE-2026-40434, CVE-2026-32650)

CVSS	Vendor	Equipment	Vulnerabilities
v3 9.8	Anviz	Anviz Multiple Products	Missing Authorization, Missing Authentication for Critical Function, Improper Neutralization of Special Elements used in a Command ('Command Injection'), Download of Code Without Integrity Check, Use of Hard-coded Cryptographic Key, Relative Path Traversal, Cleartext Transmission of Sensitive Information, Improper Verification of Source of a Communication Channel, Selection of Less-Secure Algorithm During

CVSS

Vendor

Equipment

Vulnerabilities

---

Negotiation  
(Algorithm  
Downgrade')

## Background

- **Critical Infrastructure Sectors:** Commercial Facilities, Critical Manufacturing, Defense Industrial Base, Energy, Financial Services, Food and Agriculture, Government Services and Facilities, Healthcare and Public Health, Information Technology, Transportation Systems
  - **Countries/Areas Deployed:** Worldwide
  - **Company Headquarters Location:** United States
- 

## Vulnerabilities

[Expand All +](#)

---

CVE-2026-33093



---

CVE-2026-35061



---

CVE-2026-32648



---

CVE-2026-40461



---

CVE-2026-35682



---

CVE-2026-35546



---

CVE-2026-40066



---

CVE-2026-32324



---

CVE-2026-31927



---

CVE-2026-33569



---

CVE-2026-40434



---

CVE-2026-32650

---



---

## Acknowledgments

- An anonymous researcher reported these vulnerabilities to CISA
-

# Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

---

## Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities.

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov/ics](https://www.cisa.gov/ics). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov/ics](https://cisa.gov/ics) in the technical information paper, ICS-TIP-12-146-01B-- Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

---

## Revision History

- **Initial Release Date:** 2026-04-16

Date	Revision	Summary
2026-04-16	1	Initial Publication

---

## Legal Notice and Terms of Use

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

### Tags

**Sector:** [Commercial Facilities Sector](#), [Critical Manufacturing Sector](#), [Defense Industrial Base Sector](#)

and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector>, **Energy Sector** </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/energy-sector>, **Financial Services Sector** </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector>, **Food and Agriculture Sector** </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/food-and-agriculture-sector>, **Government Services and Facilities Sector** </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-services-facilities-sector>, **Healthcare and Public Health Sector** </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector>, **Information Technology Sector** </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector>, **Transportation Systems Sector** </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector>

**Topics:** **Industrial Control System Vulnerabilities** </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, **Industrial Control Systems** </topics/industrial-control-systems>



## Please share your thoughts

We recently updated our anonymous [product survey](#); we welcome your feedback.

# Related Advisories

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-04

[Siemens Analytics Toolkit](#) </news-events/ics-advisories/icsa-26-111-04>

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-01

[Siemens TPM 2.0](#) </news-events/ics-advisories/icsa-26-111-01>

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-03

[Siemens SINEC NMS](#) </news-events/ics-advisories/icsa-26-111-03>

APR 21, 2026 ■ ICS ADVISORY | ICSA-26-111-12

[SenseLive X3050](#) </news-events/ics-advisories/icsa-26-111-12>

[Return to top](#)

[Topics](#) </topics>

[Spotlight](#) </spotlight>

[Resources & Tools](#) </resources-tools>

[News & Events](#) </news-events>

[Careers](#) </careers>

[About](#) </about>



**CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**



**CISA Central**

1-844-Say-CISA

[contact@cisa.dhs.gov](mailto:contact@cisa.dhs.gov)



CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA](#)

[Budget and Performance](#)

[DHS.gov](https://www.dhs.gov)

<https://www.dhs.gov/performance-financial-reports>

[FOIA Requests](#)

[No FEAR Act](#)

[Office of Inspector General](#)

<https://www.dhs.gov/foia>

<https://www.oig.dhs.gov/>

[Privacy Policy](#)

[Subscribe](#)

[The White House](#)

<https://www.whitehouse.gov/>

[USA.gov](https://www.usa.gov/)

[Website Feedback](#)