America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Milesight Cameras

Release Date: April 23, 2026 **Alert Code:** ICSA-26-113-03

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-26-113-03.json>

Summary

Successful exploitation of these vulnerabilities could crash the device being accessed or allow remote code execution.

The following versions of Milesight Cameras are affected:

- MS-Cxx63-PD <=51.7.0.77-r12 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)

- MS-Cxx64-xPD <=51.7.0.77-r12 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx73-xPD <=51.7.0.77-r12 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx75-xxPD <=51.7.0.77-r12 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx83-xPD <=51.7.0.77-r12 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx74-PA <=3x.8.0.3-r11 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C8477-HPG1 <=63.8.0.4-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C8477-PC <=48.8.0.4-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C5321-FPE <=62.8.0.4-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx72-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx62-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx52-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx66-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx66-xxxGPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx61-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx67-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)

- MS-Cxx71-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx41-xxxPE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx76-PE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx65-PE <=61.8.0.5-r2 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx66-xxxG1 <=63.8.0.5-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx62-xxxG1 <=63.8.0.5-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx72-xxxG1 <=63.8.0.5-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-CQxx31-xxxG1 <=CQ_63.8.0.5-r1 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-CQxx68-xxxG1 <=CQ_63.8.0.5-r1 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-CQxx72-xxxG1 <=CQ_63.8.0.5-r1 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Nxxxx-NxE <=7x.9.0.19-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Nxxxx-xxC <=7x.9.0.19-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Nxxxx-xxE <=7x.9.0.19-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Nxxxx-xxG <=7x.9.0.19-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Nxxxx-xxH <=7x.9.0.19-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)

- MS-Nxxxx-xxT <=7x.9.0.19-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- PMC8266-FPE <=PO_61.8.0.4_LPR (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- PMC8266-FGPE <=PO_61.8.0.4_LPR (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- PM3322-E <=PI_61.8.0.3_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4466-X4RIPG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS5366-X12RIPG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-X4RIPG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4466-X4RIVPG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4466-RFIVPG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-X4RIVPG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-RFIVPG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4466-X4RIWG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-X4RIWG1 <=T_63.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS5510-GVH <=T_47.8.0.4_LPR-r7 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS5510-GH <=T_47.8.0.4_LPR-r6 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)

- TS5511-GVH <=T_47.8.0.4_LPR-r6 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2966-X12TPE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4466-X4RPE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS5366-X12PE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-X4PE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2966-X12TVPE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4466-X4RVPE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS5366-X12VPE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-X4VPE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4441-X36RPE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4441-X36RE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS4466-X4RWE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-X4WE <=T_61.8.0.4_LPR-r3 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C2964-RFLPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C2972-RFLPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)

- MS-C2966-RFLWPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2866-X4TPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2866-X4TVPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2866-X4TGPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2841-X36TPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2841-X36TPC/W <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2867-X5TPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS2961-X12TPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- TS8266-FPC/P <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C2966-X12RLPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C2966-X12RLVPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C5366-X12LPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C5366-X12LVPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-C5361-X12LPC <=T_45.8.0.3-r9 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx66-xxxxGOPC <=45.8.0.2-AIoT-r4 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)

- SC211 <=C_21.1.0.8-r4 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- SP111 <=52.8.0.4-r5 (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx66-RFIPKG1 <=63.8.0.4-r1-NX (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx72-RFIPKG1 <=63.8.0.4-r1-NX (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx66-FIPKG1 <=63.8.0.4-r1-NX (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)
- MS-Cxx72-FIPKG1 <=63.8.0.4-r1-NX (CVE-2026-28747, CVE-2026-27785, CVE-2026-32644, CVE-2026-32649, CVE-2026-20766)

CVSS	Vendor	Equipment	Vulnerabilities
v3 9.8	Milesight	Milesight Cameras	Authorization Bypass Through User-Controlled Key, Use of Hard-coded Credentials, Use of Hard-coded Cryptographic Key, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Heap-based Buffer Overflow

Background

- **Critical Infrastructure Sectors:** Commercial Facilities
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** China

Vulnerabilities

Expand All +

CVE-2026-28747

CVE-2026-27785

CVE-2026-32644

CVE-2026-32649

CVE-2026-20766

Acknowledgments

- Souvik Kandar 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. 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 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.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

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

Revision History

- **Initial Release Date:** 2026-04-23

Date	Revision	Summary
2026-04-23	1	Initial Publication

Legal Notice and Terms of Use

Tags

Sector: Commercial Facilities Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/commercial-facilities-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 23, 2026 ■ ICS ADVISORY | ICSA-26-113-06

Intrado 911 Emergency Gateway (EGW) </news-events/ics-advisories/icsa-26-113-06>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-05

Hangzhou Xiongmai Technology Co., Ltd XM530 IP Camera </news-events/ics-advisories/icsa-26-113-05>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-02

Carlson Software VASCO-B GNSS Receiver </news-events/ics-advisories/icsa-26-113-02>

APR 23, 2026 ■ ICS ADVISORY | ICSA-26-113-01

Yadea T5 Electric Bicycle </news-events/ics-advisories/icsa-26-113-01>

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