Milesight Cameras Use of Hard-coded Credentials

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

Summary

CVE	CVE-2026-27785
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 00:16:23 UTC
Updated	2026-04-28 20:11:56 UTC
Description	Specific firmware versions of Milesight AIOT camera firmware contain hard-coded credentials.

Risk And Classification

Primary CVSS: v4.0 7.7 HIGH from ics-cert@hq.dhs.gov

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000150000 probability, percentile 0.029390000 (date 2026-04-28)

Problem Types: CWE-798 | CWE-798 CWE-798

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	7.7	HIGH	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/
4.0	CNA	CVSS	7.7	HIGH	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Milesight	MS-Cxx63-PD	affected 51.7.0.77-r12 custom	Not specified
CNA	Milesight	MS-Cxx64-xPD	affected 51.7.0.77-r12 custom	Not specified
CNA	Milesight	MS-Cxx73-xPD	affected 51.7.0.77-r12 custom	Not specified
CNA	Milesight	MS-Cxx75-xxPD	affected 51.7.0.77-r12 custom	Not specified
CNA	Milesight	MS-Cxx83-xPD	affected 51.7.0.77-r12 custom	Not specified

CNA	Milesight	MS-Cxx83-xPD	affected 51.7.0.77-r12 custom	Not specified
CNA	Milesight	MS-Cxx74-PA	affected 3x.8.0.3-r11 custom	Not specified
CNA	Milesight	MS-C8477-HPG1	affected 63.8.0.4-r3 custom	Not specified
CNA	Milesight	MS-C8477-PC	affected 48.8.0.4-r3 custom	Not specified
CNA	Milesight	MS-C5321-FPE	affected 62.8.0.4-r5 custom	Not specified
CNA	Milesight	MS-Cxx72-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx62-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx52-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx66-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx66-xxxGPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx61-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx67-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx71-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx41-xxxPE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx76-PE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx65-PE	affected 61.8.0.5-r2 custom	Not specified
CNA	Milesight	MS-Cxx66-xxxG1	affected 63.8.0.5-r3 custom	Not specified
CNA	Milesight	MS-Cxx62-xxxG1	affected 63.8.0.5-r3 custom	Not specified
CNA	Milesight	MS-Cxx72-xxxG1	affected 63.8.0.5-r3 custom	Not specified
CNA	Milesight	MS-CQxx31-xxxG1	affected CQ_63.8.0.5-r1 custom	Not specified
CNA	Milesight	MS-CQxx68-xxxG1	affected CQ_63.8.0.5-r1 custom	Not specified
CNA	Milesight	MS-CQxx72-xxxG1	affected CQ_63.8.0.5-r1 custom	Not specified
CNA	Milesight	MS-Nxxxx-NxE	affected 7x.9.0.19-r5 custom	Not specified
CNA	Milesight	MS-Nxxxx-xxC	affected 7x.9.0.19-r5 custom	Not specified
CNA	Milesight	MS-Nxxxx-xxE	affected 7x.9.0.19-r5 custom	Not specified
CNA	Milesight	MS-Nxxxx-xxG	affected 7x.9.0.19-r5 custom	Not specified
CNA	Milesight	MS-Nxxxx-xxH	affected 7x.9.0.19-r5 custom	Not specified
CNA	Milesight	MS-Nxxxx-xxT	affected 7x.9.0.19-r5 custom	Not specified
CNA	Milesight	PMC8266-FPE	affected PO_61.8.0.4_LPR custom	Not specified
CNA	Milesight	PMC8266-FGPE	affected PO_61.8.0.4_LPR custom	Not specified
CNA	Milesight	PM3322-E	affected PI_61.8.0.3_LPR-r3 custom	Not specified
CNA	Milesight	TS4466-X4RIPG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS5366-X12RIPG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS8266-X4RIPG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4466-X4RIVPG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4466-RFIVPG1	affected T_63.8.0.4_LPR-r3 custom	Not specified

CNA	Milesight	TS8266-X4RIVPG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS8266-RFIVPG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4466-X4RIWG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS8266-X4RIWG1	affected T_63.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS5510-GVH	affected T_47.8.0.4_LPR-r7 custom	Not specified
CNA	Milesight	TS5510-GH	affected T_47.8.0.4_LPR-r6 custom	Not specified
CNA	Milesight	TS5511-GVH	affected T_47.8.0.4_LPR-r6 custom	Not specified
CNA	Milesight	TS2966-X12TPE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4466-X4RPE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS5366-X12PE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS8266-X4PE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS2966-X12TVPE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4466-X4RVPE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS5366-X12VPE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS8266-X4VPE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4441-X36RPE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4441-X36RE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS4466-X4RWE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	TS8266-X4WE	affected T_61.8.0.4_LPR-r3 custom	Not specified
CNA	Milesight	MS-C2964-RFLPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	MS-C2972-RFLPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	MS-C2966-RFLWPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS2866-X4TPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS2866-X4TVPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS2866-X4TGPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS2841-X36TPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS2841-X36TPC/W	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS2867-X5TPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS2961-X12TPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	TS8266-FPC/P	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	MS-C2966-X12RLPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	MS-C2966-X12RLVPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	MS-C5366-X12LPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	MS-C5366-X12LVPC	affected T_45.8.0.3-r9 custom	Not specified
CNA	Milesight	MS-C5361-X12LPC	affected T_45.8.0.3-r9 custom	Not specified

CNA	Milesight	MS-Cxx66-xxxxGOPC	affected 45.8.0.2-AIoT-r4 custom	Not specified
CNA	Milesight	SC211	affected C_21.1.0.8-r4 custom	Not specified
CNA	Milesight	SP111	affected 52.8.0.4-r5 custom	Not specified
CNA	Milesight	MS-Cxx66-RFIPKG1	affected 63.8.0.4-r1-NX custom	Not specified
CNA	Milesight	MS-Cxx72-RFIPKG1	affected 63.8.0.4-r1-NX custom	Not specified
CNA	Milesight	MS-Cxx66-FIPKG1	affected 63.8.0.4-r1-NX custom	Not specified
CNA	Milesight	MS-Cxx72-FIPKG1	affected 63.8.0.4-r1-NX custom	Not specified

References

Reference	Source	Link	Tags
www.milesight.com/support/download/firmware	ics-cert@hq.dhs.gov	www.milesight.com	
www.cisa.gov/news-events/ics-advisories/icsa-26-113-03	ics-cert@hq.dhs.gov	www.cisa.gov	
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-11...	ics-cert@hq.dhs.gov	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

CNA: Souvik Kandar reported these vulnerabilities to CISA (en)

Additional Advisory Data

Solutions

CNA: Milesight advises all users to update their device to the latest firmware versions of PE/PC/PA found at https://www.milesight.com/support/download/firmware. https://www.milesight.com/support/download/firmware MS-Cxx63-PD: Update to 51.7.0.77-r13 MS-Cxx64-xPD: Update to 51.7.0.77-r13 MS-Cxx73-xPD: Update to 51.7.0.77-r13 MS-Cxx75-xxPD: Update to 51.7.0.77-r13 MS-Cxx83-xPD: Update to 51.7.0.77-r13 MS-Cxx74-PA: Update to 3x.8.0.3-r13 MS-C8477-HPG1: Update to 63.8.0.4-r4 MS-C8477-PC: Update to 48.8.0.4-r4 MS-C5321-FPE: Update to 62.8.0.4-r6 MS-Cxx72-xxxPE: Update to 61.8.0.5-r2 MS-Cxx62-xxxPE: Update to 61.8.0.5-r2 MS-Cxx52-xxxPE: Update to 61.8.0.5-r2 MS-Cxx66-xxxPE: Update to 61.8.0.5-r2 MS-Cxx66-xxxGPE: Update to 61.8.0.5-r2 MS-Cxx61-xxxPE: Update to 61.8.0.5-r2 MS-Cxx67-xxxPE: Update to 61.8.0.5-r2 MS-Cxx71-xxxPE: Update to 61.8.0.5-r2 MS-Cxx41-xxxPE: Update to 61.8.0.5-r2 MS-Cxx76-PE: Update to 61.8.0.5-r2 MS-Cxx65-PE: Update to 61.8.0.5-r2 MS-Cxx66-xxxG1: Update to 63.8.0.5-r4 MS-Cxx62-xxxG1: Update to 63.8.0.5-r4 MS-Cxx72-xxxG1: Update to 63.8.0.5-r4 MS-CQxx31-xxxG1: Update to CQ_63.8.0.5-r2 MS-CQxx68-xxxG1: Update to CQ_63.8.0.5-r2 MS-CQxx72-xxxG1: Update to CQ_63.8.0.5-r2 MS-Nxxxx-NxE: Update to 7x.9.0.19-r6 MS-Nxxxx-xxC: Update to 7x.9.0.19-r6 MS-Nxxxx-xxE: Update to 7x.9.0.19-r6 MS-Nxxxx-xxG: Update to 7x.9.0.19-r6 MS-Nxxxx-xxH: Update to 7x.9.0.19-r6 MS-Nxxxx-xxT: Update to 7x.9.0.19-r6

7x.0.0.10-10 MS-Nxxxx-xxH: Update to 7x.0.0.10-10 MS-Nxxxx-xxT: Update to 7x.0.0.10-10 PMC8266-FPE: Update to PO_61.8.0.4-r1 PMC8266-FGPE: Update to PO_61.8.0.4-r1 PM3322-E: Update to PI_61.8.0.3-r5 TS4466-X4RIPG1: Update to T_63.8.0.4-r4 TS5366-X12RIPG1: Update to T_63.8.0.4-r4 TS8266-X4RIPG1: Update to T_63.8.0.4-r4 TS4466-X4RIVPG1: Update to T_63.8.0.4-r4 TS4466-RFIVPG1: Update to T_63.8.0.4-r4 TS8266-X4RIVPG1: Update to T_63.8.0.4-r4 TS8266-RFIVPG1: Update to T_63.8.0.4-r4 TS4466-X4RIWG1: Update to T_63.8.0.4-r4 TS8266-X4RIWG1: Update to T_63.8.0.4-r4 TS5510-GVH: Update to T_47.8.0.4-r8 TS5510-GH: Update to T_47.8.0.4-r8 TS5511-GVH: Update to T_47.8.0.4-r8 TS2966-X12TPE: Update to T_61.8.0.4-r4 TS4466-X4RPE: Update to T_61.8.0.4-r4 TS5366-X12PE: Update to T_61.8.0.4-r4 TS8266-X4PE: Update to T_61.8.0.4-r4 TS2966-X12TVPE: Update to T_61.8.0.4-r4 TS4466-X4RVPE: Update to T_61.8.0.4-r4 TS5366-X12VPE: Update to T_61.8.0.4-r4 TS8266-X4VPE: Update to T_61.8.0.4-r4 TS4441-X36RPE: Update to T_61.8.0.4-r4 TS4441-X36RE: Update to T_61.8.0.4-r4 TS4466-X4RWE: Update to T_61.8.0.4-r4 TS8266-X4WE: Update to T_61.8.0.4-r4 MS-C2964-RFLPC: Update to T_45.8.0.3-r10 MS-C2972-RFLPC: Update to T_45.8.0.3-r10 MS-C2966-RFLWPC: Update to T_45.8.0.3-r10 TS2866-X4TPC: Update to T_45.8.0.3-r10 TS2866-X4TVPC: Update to T_45.8.0.3-r10 TS2866-X4TGPC: Update to T_45.8.0.3-r10 TS2841-X36TPC: Update to T_45.8.0.3-r10 TS2841-X36TPC/W: Update to T_45.8.0.3-r10 TS2867-X5TPC: Update to T_45.8.0.3-r10 TS2961-X12TPC: Update to T_45.8.0.3-r10 TS8266-FPC/P: Update to T_45.8.0.3-r10 MS-C2966-X12RLPC: Update to T_45.8.0.3-r10 MS-C2966-X12RLVPC: Update to T_45.8.0.3-r10 MS-C5366-X12LPC: Update to T_45.8.0.3-r10 MS-C5366-X12LVPC: Update to T_45.8.0.3-r10 MS-C5361-X12LPC: Update to T_45.8.0.3-r10 MS-Cxx66-xxxxGOPC: Update to 45.8.0.2-AIoT-r5 SC211: Update to C_21.1.0.8-r5 SP111: Update to 52.8.0.4-r6 MS-Cxx66-RFIPKG1: Update to 63.8.0.5-r2-NX MS-Cxx72-RFIPKG1: Update to 63.8.0.5-r2-NX MS-Cxx66-FIPKG1: Update to 63.8.0.5-r2-NX MS-Cxx72-FIPKG1: Update to 63.8.0.5-r2-NX

CNA: Milesight asks all users to report potential security vulnerabilities to security@milesight.com. mailto:security@milesight.com Learn more: Milesight Vulnerability Reporting Policy https://www.milesight.com/legal/vulnerability-report

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 registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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