Insecure generation of SAT access credentials in Ingecon EMS Board

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

Summary

CVE	CVE-2026-8072
State	PUBLISHED
Assigner	INCIBE
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 10:16:48 UTC
Updated	2026-05-13 15:36:46 UTC
Description	Insecure generation of credentials in the local SAT (Technical Support) access functionality of the Ingecon Sun EMS Board

Risk And Classification

Primary CVSS: v4.0 9.2 CRITICAL from cve-coordination@incibe.es

CVSS:4.0/AV:N/AC:H/AT:N/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: 0.000290000 probability, percentile 0.084460000 (date 2026-05-12)

Problem Types: CWE-327 | CWE-327 CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Version	Source	Type	Score	Severity	Vector
4.0	cve-coordination@incibe.es	Secondary	9.2	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/
4.0	CNA	CVSS	9.2	CRITICAL	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ingeteam	Ingecon Sun EMS Board	affected AAX1055CT custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ABU1001_P custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ACL1201_B custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ACL1200AL custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ABH1027_K custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ABH1007_Z custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ABS1009_L custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ABS1005_T custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected ACB1005_A custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	affected AAX1031CN custom	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected AAX1055CU	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ABU1001_Q	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ACL1201_C	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ACL1200AM	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ABH1027_L	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ABH1007AA	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ABS1009_P	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ABS1005_U	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected ACB1005_C	Not specified
CNA	Ingeteam	Ingecon Sun EMS Board	unaffected AAX1031CO	Not specified

References

Reference	Source	Link	Tags
www.incibe.es/en/incibe-cert/notices/aviso-sci/insecure-generation-sat-acce...	cve-coordination@incibe.es	www.incibe.es	
www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html	cve-coordination@incibe.es	www.reversemode.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

Vendor Comments And Credit

Discovery Credit

CNA: Rubén Santamarta (en)

Additional Advisory Data

Solutions

CNA: The risk has been mitigated with the release of a patch applicable to all versions, developed in December 2025. It is recommended that users update to the newer versions.

There are currently no legacy QID mappings associated with this CVE.