



# Insecure generation of SAT access credentials in Ingecon EMS Board

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

## Summary

<b>CVE</b>	CVE-2026-8072
<b>State</b>	PUBLISHED
<b>Assigner</b>	INCIBE
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-12 10:16:48 UTC
<b>Updated</b>	2026-05-13 15:36:46 UTC
<b>Description</b>	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/MSX/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/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## 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/MSX/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
<a href="http://www.incibe.es/en/incibe-cert/notices/aviso-sci/insecure-generation-sat-acce...">www.incibe.es/en/incibe-cert/notices/aviso-sci/insecure-generation-sat-acce...</a>	cve-coordination@incibe.es	<a href="http://www.incibe.es">www.incibe.es</a>	
<a href="http://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html">www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html</a>	cve-coordination@incibe.es	<a href="http://www.reversemode.com">www.reversemode.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	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.

© [CVE.report](https://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://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)