



# CVE-2017-20007

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

## Summary

<b>CVE</b>	CVE-2017-20007
<b>State</b>	PUBLIC
<b>Assigner</b>	cve-coordination@incibe.es
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-10-25 14:15:00 UTC
<b>Updated</b>	2021-10-28 20:01:00 UTC
<b>Description</b>	Ingeteam INGEPAC DA AU AUC_1.13.0.28 (and before) web application allows access to a certain path that contains sens

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Ingeteam</a>	<a href="#">Ingepac Da Au</a>	-	All	All	All
Operating System	<a href="#">Ingeteam</a>	<a href="#">Ingepac Da Au Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Information Exposure in INGEPAC DA AU   INCIBE-CERT	CONFIRM	<a href="http://www.incibe-cert.es">www.incibe-cert.es</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Industrial Cybersecurity team of S21sec, special mention to Jacinto Moral Matellán.

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

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](#) 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](#)