



# CVE-2018-17897

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

## Summary

<b>CVE</b>	CVE-2018-17897
<b>State</b>	PUBLIC
<b>Assigner</b>	ics-cert@hq.dhs.gov
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-10-17 02:29:00 UTC
<b>Updated</b>	2018-11-30 15:26:00 UTC
<b>Description</b>	LAquis SCADA Versions 4.1.0.3870 and prior has several integer overflow to buffer overflow vulnerabilities, which may allow

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lcds	Laquis Scada	All	All	All	All

## References

Reference	Source	Link	Tag
Malformed Request	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Thi
LCDS – Leão Consultoria e Desenvolvimento de Sistemas Ltda ME LAquis SCADA   ICS-CERT	MISC	<a href="http://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>	Thi
Install LAquis SCADA software	MISC	<a href="http://laquisscada.com">laquisscada.com</a>	Pro
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	car

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[590866](#) LCDS LAquis SCADA Multiple Vulnerabilities (ICSA-18-289-01)

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](#)