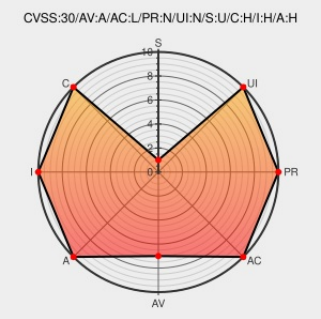
CVE-2018-17614

Published on: 11/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:19 PM UTC

CVE-2018-17614

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Arduino Mqtt Client from Losant contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Losant Arduino MQTT Client prior to V2.7. User interaction is not required to exploit this vulnerability. The specific flaw exists within the parsing of MQTT PUBLISH packets. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-6436.

CVE-2018-17614 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Losant** - **Losant Arduino MQTT Client** version **prior to V2.7**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Release v2.7 · knolleary/pubsubclient · GitHub	Release Notes github.com text/html	MISC github.com/knolleary/pubsubclient/releases/tag/v2.7
ZDI-18-1337 | Zero Day Initiative	Release Notes Third Party Advisory VDB Entry zerodayinitiative.com text/html	MISC zerodayinitiative.com/advisories/ZDI-18-1337

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Losant	Arduino Mqtt Client	All	All	All	All
Application	Losant	Arduino Mqtt Client	All	All	All	All

cpe:2.3:a:losant:arduino_mqtt_client:*:*:*:*:*:*:*:*:

cpe:2.3:a:losant:arduino_mqtt_client:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→