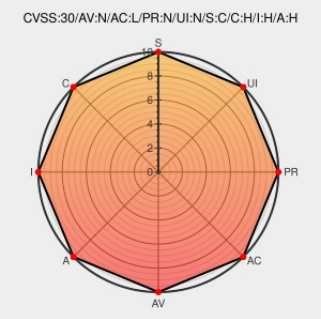
CVE-2018-19417

Published on: 11/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:41 PM UTC

CVE-2018-19417

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



Certain versions of Contiki-ng from Contiki-ng contain the following vulnerability:

An issue was discovered in the MQTT server in Contiki-NG before 4.2. The function parse_publish_vhdr() that parses MQTT PUBLISH messages with a variable length header uses memcpy to input data into a fixed size buffer. The allocated buffer can fit only MQTT_MAX_TOPIC_LENGTH (default 64) bytes, and a length check is missing. This could lead to Remote Code Execution via a stack-smashing attack (overwriting the function return address). Contiki-NG does not separate the MQTT server from other servers and the OS modules, so access to all memory regions is possible.

CVE-2018-19417 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 10 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

Stack based buffer overflow while parsing MQTT messages (parsing PUBLISH message with variable length header) · Issue #600 · contiki-ng/contiki-ng · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/contiki-ng/contiki-ng/issues/600

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Contiki-ng	Contiki-ng	All	All	All	All
Application	Contiki-ng	Contiki-ng	All	All	All	All

cpe:2.3:a:contiki-ng:contiki-ng:*:*:*:*:*:*:*:*:

cpe:2.3:a:contiki-ng:contiki-ng:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→