



CVE-2017-7653

Published on: 06/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:40 PM UTC

CVE-2017-7653

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)

CVSS:30/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

The Eclipse Mosquitto broker up to version 1.4.15 does not reject strings that are not valid UTF-8. A malicious client could cause other clients that do reject invalid UTF-8 strings to disconnect themselves from the broker by sending a topic string which is not valid UTF-8, and so cause a denial of service for the clients.

CVE-2017-7653 has been assigned by security@eclipse.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **The Eclipse Foundation - Eclipse Mosquitto** version <= 1.4.15

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
532113 – (CVE-2017-7653) CVE-2017-7653: Eclipse	Issue Tracking	CONFIRM bugs.eclipse.org/bugs/show_bug.cgi?

Mosquitto does not validate topic strings	Third Party Advisory bugs.eclipse.org text/html	id=532113
Debian -- Security Information -- DSA-4325-1 mosquitto	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4325
[SECURITY] [DLA 1525-1] mosquitto security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20180928 [SECURITY] [DLA 1525-1] mosquitto security update
	Third Party Advisory docs.oasis-open.org application/pdf	 MISC docs.oasis-open.org/mqtt/disallowed-chars/v1.0/disallowed-chars-v1.0.pdf
USN-4023-1: Mosquitto vulnerabilities Ubuntu security notices Ubuntu	usn.ubuntu.com text/html	 UBUNTU USN-4023-1

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
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Eclipse	Mosquitto	All	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:9.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:9.0:*****:						
cpe:2.3:a:eclipse:mosquitto:*****:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)