



# CVE-2016-9623

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

## Summary

<b>CVE</b>	CVE-2016-9623
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-12-12 02:59:00 UTC
<b>Updated</b>	2023-12-29 18:38:00 UTC
<b>Description</b>	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (CPU consumption) via a crafted request to the w3m web server.

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Tats</a>	<a href="#">W3m</a>	All	All	All	All
Application	<a href="#">W3m Project</a>	<a href="#">W3m</a>	All	All	All	All

## References

Reference	Source	Link	Tags
w3m/ChangeLog at master · tats/w3m · GitHub	CONFIRM	<a href="#">github.com</a>	Issue Tracking, Patch
oss-security - Re: CVE request: w3m - multiple vulnerabilities	MLIST	<a href="#">www.openwall.com</a>	Mailing List, Third Party Advice
crash after allocate string of negative size · Issue #33 · tats/w3m · GitHub	CONFIRM	<a href="#">github.com</a>	Issue Tracking, Patch
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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](#).

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