



CVE-2016-9622

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

Summary

CVE	CVE-2016-9622
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-12 02:59:00 UTC
Updated	2023-12-29 18:38:00 UTC
Description	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 crafted HTTP requests to the /w3m/ directory. The issue exists because the w3m library does not properly validate the length of the request body. This issue affects versions of w3m before 0.5.3-33.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tats	W3m	All	All	All	All
Application	W3m Project	W3m	All	All	All	All

References

Reference	Source	Link	Tags
w3m/ChangeLog at master · tats/w3m · GitHub	CONFIRM	github.com	Issue Tracking, Patch
oss-security - Re: CVE request: w3m - multiple vulnerabilities	MLIST	www.openwall.com	Mailing List, Third Party Advisory
null pointer dereference in HTMLlineproc2body · Issue #32 · tats/w3m · GitHub	CONFIRM	github.com	Issue Tracking, Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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](#)