



CVE-2017-5403

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

Summary

CVE	CVE-2017-5403
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-11 21:29:00 UTC
Updated	2018-08-07 17:42:00 UTC
Description	When adding a range to an object in the DOM, it is possible to use "addRange" to add the range to an incorrect root object.

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All

References

Reference
1340186 - (CVE-2017-5403) heap-use-after-free in nsFrameManagerBase::UndisplayedMap::RemoveNodeFor
Mozilla Firefox Multiple Bugs Let Remote Users Bypass Security Restrictions, Spoof URLs, Obtain Potentially Sensitive Information, Deny Ser
Security vulnerabilities fixed in - Thunderbird 52 — Mozilla
Mozilla Firefox CVE-2017-5403 Denial of Service Vulnerability
Security vulnerabilities fixed in Firefox 52 — Mozilla
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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