



# CVE-2017-5452

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

## Summary

<b>CVE</b>	CVE-2017-5452
<b>State</b>	PUBLIC
<b>Assigner</b>	security@mozilla.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-06-11 21:29:00 UTC
<b>Updated</b>	2018-08-09 18:12:00 UTC
<b>Description</b>	Malicious sites can display a spoofed addressbar on a page when the existing location bar on the new page is scrolled out

## Risk And Classification

**Problem Types:** CWE-20

## 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

## References

### Reference

- 1344517 - (CVE-2017-5452) Firefox for Android: Location Bar Spoofing Risk - The Location Bar remains hidden using scroll event and another
- Mozilla Firefox Multiple Bugs Let Remote Users Bypass Security Restrictions, Spoof URLs, Obtain Potentially Sensitive Information, Deny Ser
- Security vulnerabilities fixed in Firefox 53 — Mozilla
- Mozilla Firefox Multiple Security Vulnerabilities
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[690289](#) Free Berkeley Software Distribution (FreeBSD) Security Update for mozilla (5e0a038a-ca30-416d-a2f5-38cbf5e7df33)

© [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](#).

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