



# CVE-2016-5253

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

## Summary

<b>CVE</b>	CVE-2016-5253
<b>State</b>	PUBLIC
<b>Assigner</b>	security@mozilla.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-08-05 01:59:00 UTC
<b>Updated</b>	2017-08-16 01:29:00 UTC
<b>Description</b>	The Updater in Mozilla Firefox before 48.0 on Windows allows local users to write to arbitrary files via vectors involving the

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

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

## References

### Reference

92260

1246944 - (CVE-2016-5253) Arbitrary file overwrite with updater and moz maintenance service using callback application path parameter

Mozilla Firefox, Thunderbird: Multiple vulnerabilities (GLSA 201701-15) — Gentoo security

Arbitrary file manipulation by local user through Mozilla updater and callback application path parameter — Mozilla

Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Bypass Security Restrictions, Spoof Content, Modify Files, and Obtain

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

710500 Gentoo Linux Mozilla Firefox, Thunderbird Multiple Vulnerabilities (GLSA 201701-15)

© [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](#)**