



CVE-2017-5440

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

Summary

CVE	CVE-2017-5440
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 18:04:00 UTC
Description	A use-after-free vulnerability during XSLT processing due to a failure to propagate error conditions during matching while ev

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	52.0	All	All	All
Application	Mozilla	Firefox Esr	All	All	All	All
Application	Mozilla	Firefox Esr	52.0	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Application	Mozilla	Thunderbird	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference

Red Hat Customer Portal

Security vulnerabilities fixed in Thunderbird 52.1 — Mozilla

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

Security vulnerabilities fixed in Firefox ESR 45.9 — Mozilla

Red Hat Customer Portal

1336832 - (CVE-2017-5440) UAF in txExecutionState destructor during XSLT processing

Security vulnerabilities fixed in Firefox ESR 52.1 — Mozilla

Red Hat Customer Portal

Debian -- Security Information -- DSA-3831-1 firefox-esr

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378109](#) Virtuozzo Linux Security Update for thunderbird (VZLSA-2017:1201)

[378158](#) Virtuozzo Linux Security Update for thunderbird (VZLSA-2017:1201)

[378270](#) Virtuozzo Linux Security Update for firefox (VZLSA-2017:1106)

[378316](#) Virtuozzo Linux Security Update for firefox (VZLSA-2017:1104)

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

[710287](#) Gentoo Linux Mozilla Firefox Multiple Vulnerabilities (GLSA 201802-03)

© [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](#)