

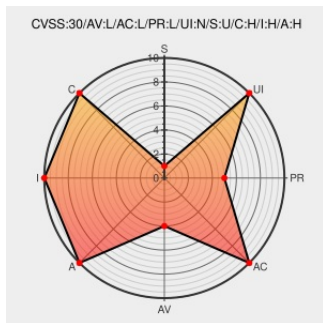


CVE-2017-7794

Published on: 06/11/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:41 PM UTC

CVE-2017-7794

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

On Linux systems, if the content process is compromised, the sandbox broker will allow files to be truncated even though the sandbox explicitly only has read access to the local file system and no write permissions. Note: This attack only affects the Linux operating system. Other operating systems are not affected. This vulnerability affects Firefox <

55.

CVE-2017-7794 has been assigned by [m](#) security@mozilla.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [m](#) **Mozilla** - **Firefox** version < 55

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Mozilla Firefox Multiple Bugs Let Remote Users Spoof Content, Obtain Potentially Sensitive Information, Deny Service and Execute Arbitrary Code - SecurityTracker

Third Party Advisory
VDB Entry
www.securitytracker.com
text/html

SECTrack 1039124

1374281 - (CVE-2017-7794) linux sandbox broker permits truncating files using read-only access

Exploit
Issue Tracking
Vendor Advisory
bugzilla.mozilla.org
text/html

CONFIRM
bugzilla.mozilla.org/show_bug.cgi?id=1374281

Security vulnerabilities fixed in Firefox 55 — Mozilla

Vendor Advisory
www.mozilla.org
text/html

CONFIRM
www.mozilla.org/security/advisories/mfsa2017-18/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

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](#).

