



CVE-2017-7844

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-7844
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-11 21:29:00 UTC
Updated	2018-08-06 17:42:00 UTC
Description	A combination of an external SVG image referenced on a page and the coloring of anchor links stored within this image car

Risk And Classification

Problem Types: CWE-200

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	Source	Li
Mozilla Firefox Flaws Lets Remote Users Obtain Potentially Sensitive Information on the Target System - SecurityTracker	SECTrack	ww
Mozilla Firefox MFSA2017-27 Multiple Security Vulnerabilities	BID	ww
Access Denied	CONFIRM	bu
Security vulnerabilities fixed in Firefox 57.0.1 — Mozilla	CONFIRM	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[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](#)