

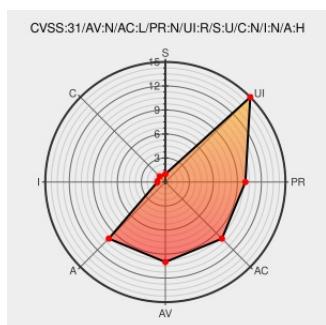


CVE-2019-11026

Published on: 04/08/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:02:00 AM UTC

CVE-2019-11026

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

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

FontInfoScanner::scanFonts in FontInfo.cc in Poppler 0.75.0 has infinite recursion, leading to a call to the error function in Error.cc.

CVE-2019-11026 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 28 Update: poppler-0.62.0-22.fc28 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-3193a75b06
[SECURITY] Fedora 30 Update: poppler-0.73.0-9.fc30 - package-announce - Fedora Mailing-Lists	Mailing List Release Notes	FEDORA FEDORA-2019-1ddce0c095

Third Party Advisory
lists.fedoraproject.org
text/html

Stack Overflow in function error (#752) · Issues · poppler / poppler · GitLab

Exploit
Issue Tracking
Third Party Advisory
gitlab.freedesktop.org
text/html

 MISC
gitlab.freedesktop.org/poppler/poppler/issues/752

[SECURITY] Fedora 29 Update: poppler-0.67.0-18.fc29 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org
text/html

 FEDORA FEDORA-2019-95eb49ef49

CVE-2019-11026: Stack-based Buffer Overflow in error () - poppler 0.75.0 - Loginsoft Research

Exploit
Third Party Advisory
research.loginsoft.com
text/html

 MISC research.loginsoft.com/bugs/1508/

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	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Freedesktop	Poppler	0.75.0	All	All	All
Application	Freedesktop	Poppler	0.75.0	All	All	All

cpe:2.3:o:fedoraproject:fedora:28:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:

cpe:2.3:a:freedesktop:poppler:0.75.0:*:*:*:*:*:

cpe:2.3:a:freedesktop:poppler:0.75.0:*:*:*:*:*:

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](#).

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