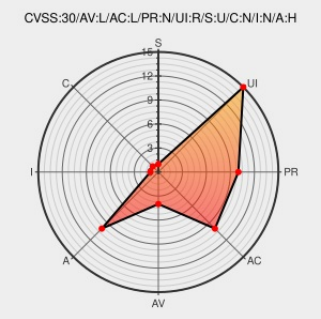
CVE-2018-19882

Published on: 12/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:39 PM UTC

CVE-2018-19882

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mupdf from Artifex contain the following vulnerability:

In Artifex MuPDF 1.14.0, the svg_run_image function in svg/svg-run.c allows remote attackers to cause a denial of service (href_att NULL pointer dereference and application crash) via a crafted svg file, as demonstrated by mupdf-gl.

CVE-2018-19882 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	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
700342 – mupdf-gl would crash while open the svg file, segmentfault	Issue Tracking, Third Party Advisory, bugs.ghostscript.com, text/html	MISC bugs.ghostscript.com/show_bug.cgi?id=700342

pocs/mupdf/20181203 at master · TeamSeri0us/pocs · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/TeamSeri0us/pocs/tree/master/mupdf/20181203
[SECURITY] Fedora 30 Update: mupdf-1.15.0-1.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-befe3bd225
[SECURITY] Fedora 29 Update: mupdf-1.15.0-1.fc29 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-15af6a9a07

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
Application	Artifex	Mupdf	1.14.0	All	All	All
Application	Artifex	Mupdf	1.14.0	All	All	All

cpe:2.3:a:artifex:mupdf:1.14.0:*:*:*:*:*:*:*

cpe:2.3:a:artifex:mupdf:1.14.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→