



CVE-2020-36280

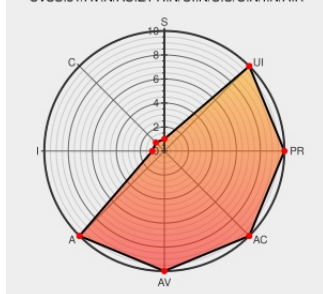
Published on: 03/11/2021 12:00:00 AM UTC

Last Modified on: 12/03/2021 05:38:00 PM UTC

CVE-2020-36280

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

Leptonica before 1.80.0 allows a heap-based buffer over-read in `pixReadFromTiffStream`, related to `tiffio.c`.

CVE-2020-36280 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 32 Update: leptonica-1.80.0-3.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-977ebc82da
Issue 23654 in oss-fuzz: Heap-	Patch	MISC

buffer-overflow in pixReadFromTiffStream · DanBloomberg/leptonica@5ba34b1 · GitHub	Third Party Advisory github.com text/html	github.com/DanBloomberg/leptonica/commit/5ba34b1fe741d69d43a6c8cf76775
[SECURITY] Fedora 33 Update: leptonica-1.80.0-3.fc33 - package- announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2021-f5f2803fff
23654 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	Exploit Third Party Advisory bugs.chromium.org text/html	 MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=23654
Leptonica: Multiple vulnerabilities (GLSA 202107-53) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202107-53
Comparing 1.79.0...1.80.0 · DanBloomberg/leptonica · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/DanBloomberg/leptonica/compare/1.79.0...1.80.0

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.

Related QID Numbers

[281062](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-f5f2803fff)

[281063](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-977ebc82da)

[281076](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-f5f2803fff)

[281077](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-977ebc82da)

[281079](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-f5f2803fff)

[281080](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-977ebc82da)

[281082](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-f5f2803fff)

[281083](#) Fedora Security Update for leptonica and mingw-leptonica (FEDORA-2021-977ebc82da)

[281329](#) Fedora Security Update for leptonica (FEDORA-2021-f5f2803fff)

[281330](#) Fedora Security Update for leptonica (FEDORA-2021-977ebc82da)

[710042](#) Gentoo Linux Leptonica Multiple Vulnerabilities (GLSA 202107-53)

Exploit/POC from Github

PoC for exploiting CVE-2020-36280 : Leptonica before 1.80.0 allows a heap-based buffer over-read in pixReadFromTiffSt...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Leptonica	Leptonica	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:						
cpe:2.3:a:leptonica:leptonica:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title				Posted (UTC)	

← Previous ID

Next ID →