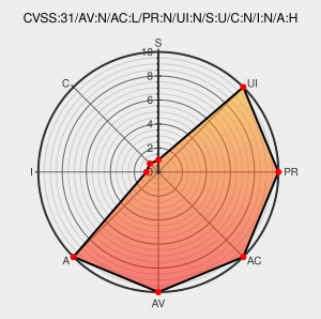
CVE-2020-36277

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

Last Modified on: 12/03/2021 05:37:00 PM UTC

CVE-2020-36277

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

Leptonica before 1.80.0 allows a denial of service (application crash) via an incorrect left shift in pixConvert2To8 in pixconv.c.

CVE-2020-36277 has been assigned by 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
[SECURITY] [DLA 2612-1] leptonlib security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20210331 [SECURITY] [DLA 2612-1] leptonlib security update

[SECURITY] Fedora 33 Update: leptonica-1.80.0-3.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-f5f2803fff
Fix heap buffer overflow in selReadStream (detected by clang address sanitizer) by stweil · Pull Request #499 · DanBloomberg/leptonica · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/DanBloomberg/leptonica/pull/499
Leptonica: Multiple vulnerabilities (GLSA 202107-53) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202107-53
21997 - 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=21997
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

Related QID Numbers

178488 Debian Security Update for leptonlib (DLA 2612-1)

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-2020-36277 : Leptonica before 1.80.0 allows a denial of service (application crash) via an inc…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Leptonica	Leptonica	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:33:*:*:*:*:*:*:*:

cpe:2.3:a:leptonica:leptonica:*:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@vigilance_fr	Vigil@nce #Vulnérabilité de leptonlib : quatre vulnérabilités. vigilance.fr/vulnerabilite/… Références : #CVE-2020-36277… twitter.com/i/web/status/1…	2021-03-31 20:09:03
@vigilance_en	Vigil@nce #Vulnerability of leptonlib: four vulnerabilities. vigilance.fr/vulnerability/… Identifiers: #CVE-2020-36277,… twitter.com/i/web/status/1…	2021-03-31 20:09:04

← Previous ID

Next ID→