



CVE-2021-45943

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-45943
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-01 01:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	GDAL 3.3.0 through 3.4.0 has a heap-based buffer overflow in PCIDSK::CPCIDSKFile::ReadFromFile (called from PCIDSK

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Oracle	Spatial And Graph	19c	All	All	All
Application	Oracle	Spatial And Graph	21c	All	All	All
Application	Osgeo	Gdal	All	All	All	All

References

Reference
PCIDSK: fix write heap-buffer-overflow. Fixes https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=41993 by rouault · Pull Request #4944 · C
[SECURITY] Fedora 34 Update: gdal-3.2.2-3.fc34 - package-announce - Fedora Mailing-Lists
oss-fuzz-vulns/OSV-2021-1651.yaml at main · google/oss-fuzz-vulns · GitHub
Merge pull request #4944 from rouault/fix_ossfuzz_41993 · OSGeo/gdal@1ca6a3e · GitHub
[SECURITY] [DLA 2877-1] gdal security update
41993 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail

[SECURITY] Fedora 35 Update: mingw-gdal-3.3.3-3.fc35 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 3129-1] gdal security update

[SECURITY] Fedora 35 Update: mingw-gdal-3.3.3-3.fc35 - package-announce - Fedora Mailing-Lists

Debian -- Security Information -- DSA-5239-1 gdal

[SECURITY] Fedora 34 Update: gdal-3.2.2-3.fc34 - package-announce - Fedora Mailing-Lists

Oracle Critical Patch Update Advisory - July 2022

GDAL: Heap Buffer Overflow (GLSA 202210-15) — Gentoo security

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178998](#) Debian Security Update for gdal (DLA 2877-1)

[181079](#) Debian Security Update for gdal (DSA 5239-1)

[181087](#) Debian Security Update for gdal (DLA 3129-1)

[182088](#) Debian Security Update for gdal (CVE-2021-45943)

[20262](#) Oracle Database 21c Critical Patch Update - July 2022

[20263](#) Oracle Database 19c Critical Patch Update - July 2022

[20274](#) Oracle Database 19c Critical OJVM Patch Update - July 2022

[282562](#) Fedora Security Update for gdal (FEDORA-2022-e85e37206b)

[282564](#) Fedora Security Update for gdal (FEDORA-2022-cffc5dbf4)

[710668](#) Gentoo Linux GDAL Heap Buffer Overflow Vulnerability (GLSA 202210-15)

© [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](#)