



CVE-2005-2958

Published on: 10/25/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:29 PM UTC

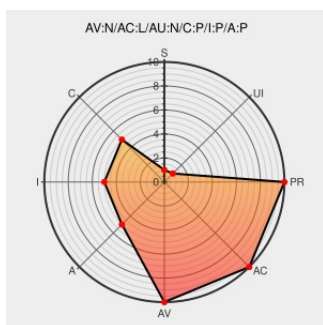
CVE-2005-2958

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Libgda2](#) from [Gnome](#) contain the following vulnerability:

Multiple format string vulnerabilities in the GNOME Data Access library for GNOME2 (libgda2) 1.2.1 and earlier allow attackers to execute arbitrary code.

CVE-2005-2958 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Secunia - Advisories - Ubuntu update for libgda2-1 / libgda2-3

[web.archive.org](#)
[text/html](#)

[SECUNIA 17391](#)

Security Announcement

[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[SUSE SUSE-SR:2005:027](#)

Secunia - Advisories - Fedora update for libgda

[web.archive.org](#)
[text/html](#)

[SECUNIA 17500](#)

Secunia - Advisories - Gentoo update for libgda

[web.archive.org](#)
[text/html](#)

[SECUNIA 17426](#)

Advisories - Mandriva

[www.mandriva.com](#)
[text/html](#)

[MANDRIVA MDKSA-2005:203](#)

SecurityTracker.com Archives - libgda2 Format String Bugs May Let Users Execute

[securitytracker.com](#)

[SECTRAK 1015107](#)

Arbitrary Code	text/html	
Secunia - Advisories - GNOME-DB libgda Logging Functions Format String Vulnerabilities	web.archive.org text/html	 SECUNIA 17323
Secunia - Advisories - SUSE Updates for Multiple Packages	web.archive.org text/html	 SECUNIA 17559
USN-212-1: libgda2 vulnerability Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-212-1
Gentoo Linux Documentation -- libgda: Format string vulnerabilities	www.gentoo.org text/html	 GENTOO GLSA-200511-01
LibGDA Multiple Format String Vulnerabilities	cve.report (archive) text/html	 BID 15200
[SECURITY] Fedora Core 3 Update: libgda-1.0.4-3.1	www.redhat.com text/html	 FEDORA FEDORA-2005-1029
Secunia - Advisories - Debian update for libgda2	web.archive.org text/html	 SECUNIA 17339
Debian -- Security Information -- DSA-871-2 libgda2	Patch Vendor Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-871

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	Gnome	Libgda2	All	All	All	All
cpe:2.3:a:gnome:libgda2:*:*:*:*:*:						

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](#)