

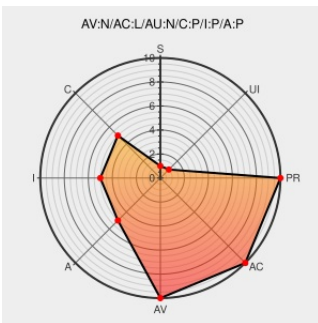


CVE-2005-1100

Published on: 04/13/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1100

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

Certain versions of [Gld](#) from [Salim Gasmi](#) contain the following vulnerability:

Format string vulnerability in the ErrorLog function in cnf.c in Greylisting daemon (GLD) 1.3 and 1.4 allows remote attackers to execute arbitrary code via format string specifiers in data that is passed directly to syslog.

CVE-2005-1100 has been assigned by [M](#) cve@mitre.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

'GLD (Greylisting daemon for Postfix) multiple vulnerabilities.' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20050412 GLD](#)
(Greylisting daemon for
Postfix) multiple vulnerabilities.

Gentoo Linux Documentation -- Gld: Remote execution of arbitrary code

[Patch](#)
[security.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-200504-10](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF gld-cnfc-format-string\(20067\)](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 15493](#)

Inactive Link **Not Archived**

Secunia - Advisories - Gld Multiple Vulnerabilities

[Patch](#)
[web.archive.org](#)

[SECUNIA 14941](#)

[text/html](#)

SecurityTracker.com Archives - Gld Format String Flaws and Buffer Overflows Let Remote Users Execute Arbitrary Code With Root Privileges

[securitytracker.com](#)[SECTrack 1013678](#)[text/html](#)

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	Salim Gasmi	Gld	1.3	All	All	All
Application	Salim Gasmi	Gld	1.4	All	All	All
Application	Salim Gasmi	Gld	1.3	All	All	All
Application	Salim Gasmi	Gld	1.4	All	All	All
cpe:2.3:a:salim_gasmi:gld:1.3:*****:						
cpe:2.3:a:salim_gasmi:gld:1.4:*****:						
cpe:2.3:a:salim_gasmi:gld:1.3:*****:						
cpe:2.3:a:salim_gasmi:gld:1.4:*****:						

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](#)