

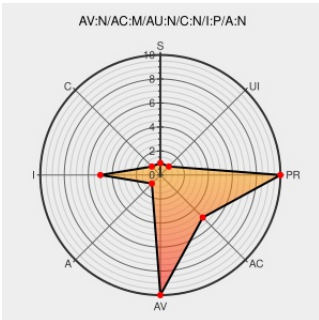


CVE-2014-100030

Published on: 01/13/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:48 PM UTC

CVE-2014-100030

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

Certain versions of [Ganesha Digital Library](#) from [Ganesha Digital Library Project](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in module/search/function.php in Ganesha Digital Library (GDL) 4.2 allows remote attackers to inject arbitrary web script or HTML via the keyword parameter in a ByEge action.

CVE-2014-100030 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF ganesha-gdl-xss\(91553\)](#)

GDL 4.2 XSS / SQL Injection / Traversal ≈ Packet Storm

[Exploit](#)
[packetstormsecurity.com](#)
[text/html](#)

[MISC](#)
[packetstormsecurity.com/files/125464](#)

Security Advisory SA57171 - Ganesha Digital Library Cross-Site Scripting and SQL Injection Vulnerabilities - Secunia

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

[SECUNIA 57171](#)

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	Ganesha Digital Library Project	Ganesha Digital Library	4.2	All	All	All
Application	Ganesha Digital Library Project	Ganesha Digital Library	4.2	All	All	All
cpe:2.3:a:ganesha_digital_library_project:ganesha_digital_library:4.2:*:*:*:*:*:						
cpe:2.3:a:ganesha_digital_library_project:ganesha_digital_library:4.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)