



CVE-2015-7314

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

Summary

CVE	CVE-2015-7314
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-06 01:59:00 UTC
Updated	2015-10-07 14:45:00 UTC
Description	The Precious module in gollum before 4.0.1 allows remote attackers to read arbitrary files by leveraging the lack of a certain

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gollum Project	Gollum	All	All	All	All

References

Reference	Source	Link
JVNDB-2015-000149	JVNDB	jvndb.jvn.jp
Added security check. · gollum/gollum@ce68a88 · GitHub	CONFIRM	github.com
oss-security - Re: CVE Request: gollum information disclosure vulnerability	MLIST	www.openwal
[SECURITY] [FIXED] Information disclosure vulnerability, please update! · Issue #1070 · gollum/gollum · GitHub	CONFIRM	github.com
JVN#27548431: gollum vulnerable to file exposure	JVN	jvn.jp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)