



CVE-2016-15005

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

Summary

CVE	CVE-2016-15005
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-27 22:15:00 UTC
Updated	2023-02-28 18:15:00 UTC
Description	CSRF tokens are generated using math/rand, which is not a cryptographically secure random number generator, allowing a

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Merge pull request #24 from bentranter/use-crypto-rand-for-xsrf · dinever/golf@3776f33 · GitHub	MISC	github.com	
GO-2020-0045 - Go Packages	MISC	pkg.go.dev	
Use crypto/rand for XSRF token generation by bentranter · Pull Request #24 · dinever/golf · GitHub	MISC	github.com	
Use crypto/rand instead of math/rand · Issue #20 · dinever/golf · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

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