CVE-2014-7189

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-7189
State	PUBLISHED
Assigner	canonical
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-07 14:55:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	crpyto/tls in Go 1.1 before 1.3.2, when SessionTicketsDisabled is enabled, allows man-in-the-middle attackers to spoof clie

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	1.1	All	All	All

Application	Golang	Go	1.1.1	All	All	All
Application	Golang	Go	1.1.2	All	All	All
Application	Golang	Go	1.2	All	All	All
Application	Golang	Go	1.2.1	All	All	All
Application	Golang	Go	1.2.2	All	All	All
Application	Golang	Go	1.3	All	All	All
Application	Golang	Go	1.3.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Google Groups	af854a3a-2127-422b-91ae-364da2661108	groups.google.com
Go TLS Server Implementation Security Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com
oss-security - Re: CVE Request: Go crypto/tls vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com
Google Groups	MITRE	groups.google.com
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.