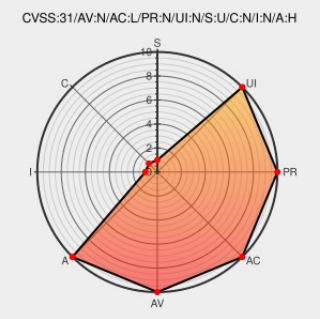
CVE-2013-10005

Published on: Not Yet Published

Last Modified on: 02/28/2023 06:07:19 PM UTC

CVE-2013-10005

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Socks5 from Socks5 Project contain the following vulnerability:

The RemoteAddr and LocalAddr methods on the returned net.Conn may call themselves, leading to an infinite loop which will crash the program due to a stack overflow.

CVE-2013-10005 has been assigned by security@golang.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **github.com/btcsuite/go-socks** - **github.com/btcsuite/go-socks** version **< 0.0.0-20130808000456-233bccbb1abe**

Affected Vendor/Software: **github.com/btcsuitereleases/go-socks** - **github.com/btcsuitereleases/go-socks** version **< 0.0.0-20130808000456-233bccbb1abe**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
GO-2020-0024 - Go Packages	pkg.go.dev text/html	MISC pkg.go.dev/vuln/GO-2020-0024
fix potential infinite loops in both LocalAddr and RemoteAddr · btcsuite/go-socks@233bccb · GitHub	github.com text/html	MISC github.com/btcsuite/go-socks/commit/233bccbb1abe02f05750f7ace66f5bffdb13defc

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	Socks5 Project	Socks5	All	All	All	All

cpe:2.3:a:socks5_project:socks5:*:*:*:*:*:go:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report