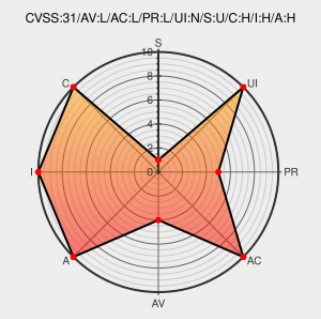
CVE-2016-3958

Published on: 05/23/2016 12:00:00 AM UTC

Last Modified on: 08/16/2022 01:18:00 PM UTC

CVE-2016-3958

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



Certain versions of Go from Golang contain the following vulnerability:

Untrusted search path vulnerability in Go before 1.5.4 and 1.6.x before 1.6.1 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, related to use of the LoadLibrary function.

CVE-2016-3958 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Gerrit Code Review	go-review.googlesource.com text/html	CONFIRM go-review.googlesource.com/#/c/21428/
syscall: guard against Windows DLL preloading attacks · Issue #14959 · golang/go · GitHub	Vendor Advisory github.com	CONFIRM github.com/golang/go/issues/14959

	text/html	
Google Groups	groups.google.com text/html	MLIST [golang-announce] 20160412 [security] Go 1.6.1 and 1.5.4 are released
oss-security - Re: CVE request - Go - DLL loading, Big int	www.openwall.com text/html	MLIST [oss-security] 20160405 Re: CVE request - Go - DLL loading, Big int
oss-security - CVE request - Go - DLL loading, Big int	www.openwall.com text/html	MLIST [oss-security] 20160405 CVE request - Go - DLL loading, Big int

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	Golang	Go	All	All	All	All
Application	Golang	Go	1.6	All	All	All
Application	Golang	Go	1.6	All	All	All
Application	Golang	Go	All	All	All	All

cpe:2.3:a:golang:go:*:*:*:*:*:*:*:*:

cpe:2.3:a:golang:go:1.6:*:*:*:*:*:*:*:

cpe:2.3:a:golang:go:1.6:*:*:*:*:*:*:*:

cpe:2.3:a:golang:go:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→