



# CVE-2017-15041

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-15041
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-10-05 21:29:00 UTC
<b>Updated</b>	2021-03-19 20:11:00 UTC
<b>Description</b>	Go before 1.8.4 and 1.9.x before 1.9.1 allows "go get" remote command execution. Using custom domains, it is possible to

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	1.9	All	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	1.9	-	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	1.9	All	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Developer Tools</a>	1.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Tus</a>	7.7	All	All	All

## References

Reference	Source	Link
[SECURITY] [DLA 2591-1] golang-1.7 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>

[SECURITY] [DLA 2592-1] golang-1.8 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Google Groups	CONFIRM	<a href="https://groups.google.com">groups.google.com</a>
Go: Multiple vulnerabilities (GLSA 201710-23) — Gentoo Security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
Golang Go CVE-2017-15041 Remote Code Execution Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
<a href="https://golang.org/cl/68022">golang.org/cl/68022</a>	CONFIRM	<a href="https://golang.org">golang.org</a>
<a href="https://golang.org/cl/68190">golang.org/cl/68190</a>	CONFIRM	<a href="https://golang.org">golang.org</a>
cmd/go: arbitrary code execution during “go get” or “go get -d” [Go 1.8] · Issue #22125 · golang/go · GitHub	CONFIRM	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)

[710511](#) Gentoo Linux Go Multiple Vulnerabilities (GLSA 201710-23)

© [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](#).

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