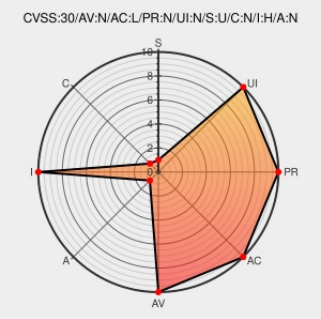
CVE-2017-18367

Published on: 04/24/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18367

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



Certain versions of Libseccomp-golang from Libseccomp-golang Project contain the following vulnerability:

libseccomp-golang 0.9.0 and earlier incorrectly generates BPFs that OR multiple arguments rather than ANDing them. A process running under a restrictive seccomp filter that specified multiple syscall arguments could bypass intended access restrictions by specifying a single matching argument.

CVE-2017-18367 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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	HIGH	NONE

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	REDHAT RHSA-2019:4090
BUG: Handling of multiple syscall arguments	Patch	MISC github.com/seccomp/libseccomp-golang/issues/22

BUG: Handling of multiple syscall arguments incorrect (CVE-2017-18367) · Issue #22 · seccomp/libseccomp-golang · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/seccomp/libseccomp-golang/issues/22
USN-4574-1: libseccomp-golang vulnerability | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4574-1
golang: Resolve bug with handling of multiple argument rules · seccomp/libseccomp-golang@06e7a29 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/seccomp/libseccomp-golang/commit/06e7a29f36a34b8cf419aeb87b979ee508e58f9e
oss-security - Re: CVE Request: golang-seccomp incorrectly handles multiple syscall arguments	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20190425 Re: CVE Request: golang-seccomp incorrectly handles multiple syscall arguments
[SECURITY] [DLA 2320-1] golang-github-seccomp-libseccomp-golang security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200811 [SECURITY] [DLA 2320-1] golang-github-seccomp-libseccomp-golang security update
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	REDHAT RHSA-2019:4087

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.

Related QID Numbers

770012 Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2019:4087)

982573 Go (go) Security Update for github.com/seccomp/libseccomp-golang (GHSA-58v3-j75h-xr49)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libseccomp-golang Project	Libseccomp-golang	All	All	All	All

cpe:2.3:a:libseccomp-golang_project:libseccomp-golang:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→