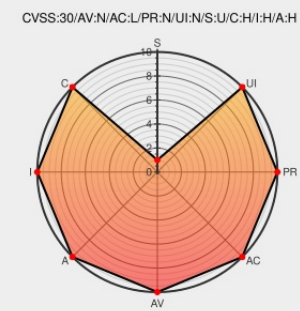
CVE-2019-9893

Published on: 03/20/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:08 PM UTC

CVE-2019-9893

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



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

libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might able to lead to bypassing seccomp filters and potential privilege escalations.

CVE-2019-9893 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
BUG: 64-bit argument comparisons do not work correctly (CVE-2019-9893) · Issue #139 · seccomp/libseccomp · GitHub	Patch, github.com, text/html	MISC github.com/seccomp/libseccomp/issues/139
libseccomp: Privilege escalation (GLSA 201904-18) — Gentoo security	security.gentoo.org	GENTOO GLSA-201904-18

	text/html	
USN-4001-1: libseccomp vulnerability | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4001-1
[security-announce] openSUSE-SU-2019:2283-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2019:2283
USN-4001-2: libseccomp vulnerability | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4001-2
[security-announce] openSUSE-SU-2019:2280-1: moderate: Security update f	lists.opensuse.org text/html	SUSE openSUSE-SU-2019:2280
oss-sec: libseccomp: incorrect generation of syscall argument filters	Mailing List Patch Third Party Advisory seclists.org text/html	MISC seclists.org/oss-sec/2019/q1/179
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:3624

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

500310 Alpine Linux Security Update for libseccomp

710167 Gentoo Linux libseccomp Privilege escalation Vulnerability (GLSA 201904-18)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:libseccomp_project:libseccomp:*:*:*:*:*:*:*:*:

cpe:2.3:a:libseccomp_project:libseccomp:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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