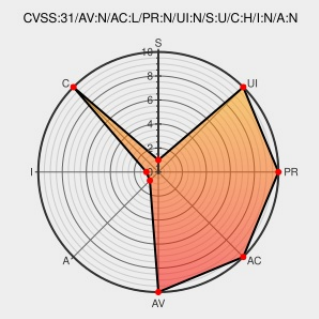
CVE-2020-29050

Published on: 01/07/2022 12:00:00 AM UTC

Last Modified on: 04/01/2022 03:19:00 PM UTC

CVE-2020-29050

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

SphinxSearch in Sphinx Technologies Sphinx through 3.1.1 allows directory traversal (in conjunction with CVE-2019-14511) because the mysql client can be used for CALL SNIPPETS and load_file operations on a full pathname (e.g., a file in the /etc directory). NOTE: this is unrelated to CMUSphinx.

CVE-2020-29050 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	HIGH	NONE	NONE

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2020-29050	security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2020-29050
[SECURITY] [DLA 2882-1] sphinxsearch	lists.debian.org	MLIST [debian-lts-announce] 20220117 [SECURITY] [DLA

security update	text/html	2882-1] sphinxsearch security update
SphinxSearch 0.0.0.0:9306 (CVE-2019-14511) » we got style	blog.wirhabenstil.de text/html	MISC blog.wirhabenstil.de/2019/08/19/sphinxsearch-0-0-0-09306-cve-2019-14511/

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

178987 Debian Security Update for sphinxsearch (DSA 5036-1)

179007 Debian Security Update for sphinxsearch (DLA 2882-1)

751738 OpenSUSE Security Update for sphinx (openSUSE-SU-2022:0046-1)

751770 OpenSUSE Security Update for sphinx (openSUSE-SU-2022:0054-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Sphinxsearch	Sphinx	All	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:sphinxsearch:sphinx:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-29050 : SphinxSearch in Sphinx Technologies Sphinx through 3.1.1 allows directory traversal in conjunctio… twitter.com/i/web/status/1…	2022-01-07 07:02:08
@SecRiskRptSME	RT: CVE-2020-29050 SphinxSearch in Sphinx Technologies Sphinx through 3.1.1 allows directory traversal (in conjunc… twitter.com/i/web/status/1…	2022-01-07 08:33:37
/r/netcve	CVE-2020-29050	2022-01-07 07:38:02

← Previous ID

Next ID→

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