Aug
19
2019

SphinxSearch 0.0.0.0:9306 (CVE-2019-14511)

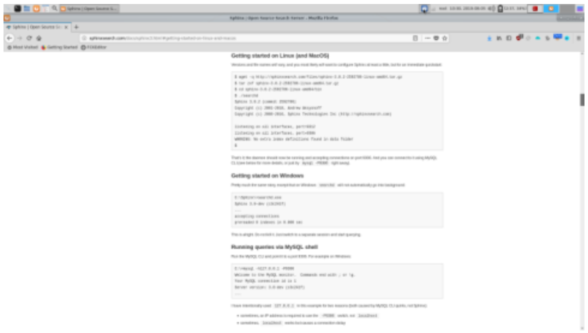
Uncategorized Add comments

TL;DR: SphinxSearch comes with a insecure default configuration that opens a listener on port 9306. No auth required. Connections using a mysql client are possible.

I recently stumbled upon SphinxSearch. A fast database that can do full-text search much faster than MySQL/MariaDB (at least in my scenario) and runs on lower ressources than Lucene, Solr or Elasticsearch (which also performed the worst in my scenario).

One thing I came accross while installing it was the default configuration. In the default configuration SphinxSearch has a listener on TCP port 9306 with no authentication. Actually authentication is not implemented in SphinxSearch as far as I know. This would make you think that this listener is at least limited to localhost? Nope. The default setup creates a listener on 0.0.0.0:9306 (reading all interfaces, any IP port 9306) and allows connections without credentials using the MySQL client.

This is a screenshot from the official documentation as of August 2019:



Getting started on Linux (and MacOS)

Getting started on Windows

Running queries via MySQL shell

“Archive” screenshot

I have tried contacting the SphinxSearch team using the website form and via Skype since July, but no reply.

How to fix it?
Just go to your SphinxSearch configuration and edit the listen variable to include only localhost or put a (host) firewall like iptables in front of your installation.

Sample of a localhost listener configuration:

```
[..]
searchd
 {
         listen                  = localhost:9312
         listen                  = localhost:9306:mysql41
[..]
```

At the time of writing the Internet has 100+ exposed installations. Some of them might be on purpose or the data might not be a secret, but for some it might be an issue. I know at least one project for email archiving which uses SphinxSearch – piler. Users should check it immediately.

This is an example of a SphinxSearch login using mysqlclient:

```
root@vmd292 ~/sphinx/sphinx-3.1.1/bin # mysql -P9306 -h127.0.0.1
 Welcome to the MariaDB monitor.  Commands end with ; or \g.
 Your MySQL connection id is 1
 Server version: 3.1.1 (commit 612d99f) Copyright (c) 2000, 2018,
Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MySQL [(none)]&gt; show tables;

+---------------+-------------+

| Index         | Type        |

+---------------+-------------+

| idx1_template | local       |

| idx1p0        | local       |

| idx1p1        | local       |

| idx1p10       | local       |

| idx1p11       | local       |

| idx1p12       | local       |
```

Archives

- November 2022 (1)
- October 2022 (2)
- June 2022 (3)
- April 2022 (5)
- March 2022 (1)
- February 2022 (1)
- January 2022 (1)
- December 2021 (2)
- November 2021 (1)
- September 2021 (1)
- August 2021 (3)
- July 2021 (1)
- April 2021 (2)
- February 2021 (2)
- January 2021 (1)
- December 2020 (6)
- October 2020 (1)
- July 2020 (1)
- June 2020 (1)
- May 2020 (1)
- December 2019 (2)
- August 2019 (2)
- April 2019 (2)
- March 2019 (1)
- August 2018 (1)
- July 2018 (1)
- November 2016 (5)
- September 2016 (2)
- May 2016 (3)
- February 2016 (6)
- January 2016 (2)
- October 2015 (2)
- September 2015 (2)
- August 2015 (2)
- January 2015 (4)
- November 2014 (1)
- October 2014 (1)
- September 2014 (1)
- August 2014 (4)
- July 2014 (3)
- June 2014 (1)
- May 2014 (1)
- April 2014 (6)
- February 2014 (8)
- January 2014 (6)
- December 2013 (2)
- November 2013 (1)
- September 2013 (6)
- August 2013 (2)
- May 2013 (1)
- April 2013 (8)
- September 2012 (4)
- August 2012 (12)
- July 2012 (3)
- June 2012 (8)
- May 2012 (2)
- April 2012 (4)
- March 2012 (6)
- February 2012 (6)
- January 2012 (6)
- September 2011 (3)
- August 2011 (1)
- July 2011 (2)
- May 2011 (3)

Recent Posts

- Owncloud password reset returns 503 and fails (fix) 12/11/2022
- Changing your AWS password from the CLI 26/10/2022
- Azure storage signature parameters explained 11/10/2022
- Get Bluetooth battery level in Linux (specifically Ubuntu) 12/06/2022
- Sublime Text Hotkey to mark some lines as comment 10/06/2022
- Wireguard tunnel all, but allow local network access? 08/06/2022

```
| idx1p13       | local       |

| idx1p14       | local       |

| idx1p15       | local       |

| idx1p16       | local       |

| idx1p17       | local       |

| idx1p18       | local       |

| idx1p19       | local       |

| idx1p2        | local       |

| idx1p20       | local       |

| idx1p3        | local       |

| idx1p4        | local       |

| idx1p5        | local       |

| idx1p6        | local       |

| idx1p7        | local       |

| idx1p8        | local       |

| idx1p9        | local       |

| test1         | distributed |

+---------------+-------------+

23 rows in set (0.001 sec)
MySQL [(none)]&gt; quit
 Bye
 root@vmd292 ~/sphinx/sphinx-3.1.1/bin #
```

Posted by adminze at 17:00

3 Responses to “SphinxSearch 0.0.0.0:9306 (CVE-2019-14511)”

1. **Sergey Nikolaev** says:
   21/08/2019 at 03:11

   Hi. Thanks for pointing this out. We're making a fork of Sphinx Search – much better supported, with monthly releases, new features (replication, PQ indexes etc.) and so on.
   We've discussed it with the team and decided to update the defaults. Here's the issue
   https://github.com/manticoresoftware/manticoresearch/issues/261

   BTW in terms of security we have 2 more things:
   – SSL support for http (already on github, should be released in beta stage in few days)
   – another vulnerability fixed – CALL SNIPPETS() could let you read any file from the OS.
   https://docs.manticoresearch.com/latest/singlehtml/index.html#snippets-file-prefix fixes it. Together with the listens at 0.0.0.0 by default may be quite a breach in Sphinx.

   We'll appreciate if you ping us in case you find anything else in Sphinx/Manticore. Follow us on https://twitter.com/manticoresearch, come to our http://slack.manticoresearch.com, https://forum.manticoresearch.com and post issues on https://github.com/manticoresoftware/manticoresearch/issues

   Reply

   adminze says:
   29/08/2019 at 09:08

   Awesome, thanks a lot for the information! I didnt know about Manticoresearch, only Sphinx. I will give it a try!

   CALL SNIPPETS() sounds interesting and scary at the same time…

   Reply

2. **Sergey Nikolaev** says:
   23/08/2019 at 05:26

   https://github.com/manticoresoftware/manticoresearch/issues/261 has been fixed.

   Reply

Leave a Reply

Your Comment

TP-Link CPE210 Pharos Access Point pentest fun 25/04/2022
curl compressed returning answer, otherwise empty 22/04/2022
Home Assistant Life Hacks 15/04/2022
Compile mimikatz 08/04/2022

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name (required)

E-mail (required)

URI

□

Save my name, email, and website in this browser for the next time I comment.

Submit Comment

Lotus Domino Password retrival

Powershell script to see failed logins in AD

Suffusion theme by Sayontan Sinha