



# CVE-2018-10850

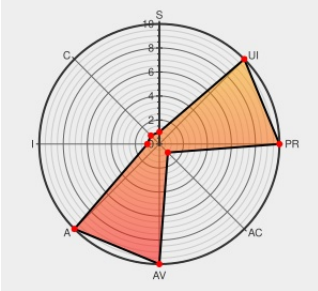
Published on: 06/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

## CVE-2018-10850

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

389-ds-base before versions 1.4.0.10, 1.3.8.3 is vulnerable to a race condition in the way 389-ds-base handles persistent search, resulting in a crash if the server is under load. An anonymous attacker could use this flaw to trigger a denial of service.

CVE-2018-10850 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **[UNKNOWN]** - 389-ds-base version 389-ds-base 1.4.0.10

Affected Vendor/Software: **[UNKNOWN]** - 389-ds-base version 389-ds-base 1.3.8.3

CVSS3 Score: **5.9 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.1 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>COMPLETE</b>     |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

|                                                                                                                                   |                                                                                                                                            |                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| [SECURITY] [DLA 1428-1] 389-ds-base security update                                                                               | <a href="#">Third Party Advisory</a><br><a href="#">lists.debian.org</a><br><a href="#">text/html</a>                                      | <a href="#">MLIS I [debian-its-announce] 20180/15 [SECURITY] [DLA 1428-1] 389-ds-base security update</a> |
| [security-announce] openSUSE-SU-2019:1397-1: important: Security update                                                           | <a href="#">lists.opensuse.org</a><br><a href="#">text/html</a>                                                                            | <a href="#">SUSE openSUSE-SU-2019:1397</a>                                                                |
| Issue #49768: Under network intensive load persistent search can erroneously decrease connection refcnt - 389-ds-base - Pagure.io | <a href="#">Issue Tracking</a><br><a href="#">Third Party Advisory</a><br><a href="#">pagure.io</a><br><a href="#">text/html</a>           | <a href="#">CONFIRM pagure.io/389-ds-base/issue/49768</a>                                                 |
| 1588056 – (CVE-2018-10850) CVE-2018-10850 389-ds-base: race condition on reference counter leads to DoS using persistent search   | <a href="#">Issue Tracking</a><br><a href="#">Third Party Advisory</a><br><a href="#">bugzilla.redhat.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10850</a>                                |
| Red Hat Customer Portal                                                                                                           | <a href="#">Third Party Advisory</a><br><a href="#">access.redhat.com</a><br><a href="#">text/html</a>                                     | <a href="#">REDHAT RHSA-2018:2757</a>                                                                     |
| Commit - 389-ds-base - 8f04487f99a - Pagure.io                                                                                    | <a href="#">Patch</a><br><a href="#">Third Party Advisory</a><br><a href="#">pagure.io</a><br><a href="#">text/html</a>                    | <a href="#">CONFIRM pagure.io/389-ds-base/c/8f04487f99a</a>                                               |

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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type             | Vendor                        | Product                                  | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a>             | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a>             | 8.0     | All    | All     | All      |
| Application      | <a href="#">Fedoraproject</a> | <a href="#">389 Directory Server</a>     | All     | All    | All     | All      |
| Application      | <a href="#">Fedoraproject</a> | <a href="#">389 Directory Server</a>     | All     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux</a>         | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux</a>         | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux Desktop</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux Desktop</a> | 7.0     | 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</a>  | 7.0     | All    | All     | All      |

|                                                            |        |                              |     |     |     |     |
|------------------------------------------------------------|--------|------------------------------|-----|-----|-----|-----|
| Operating System                                           | Redhat | Enterprise Linux Server Aus  | 7.6 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Server Aus  | 7.6 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Server Eus  | 7.5 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Server Eus  | 7.6 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Server Eus  | 7.5 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Server Eus  | 7.6 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Server Tus  | 7.6 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Server Tus  | 7.6 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System                                           | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| cpe:2.3:o:debian:debian_linux:8.0:****:*:*:                |        |                              |     |     |     |     |
| cpe:2.3:o:debian:debian_linux:8.0:****:*:*:                |        |                              |     |     |     |     |
| cpe:2.3:a:fedoraproject:389_directory_server:****:*:*:     |        |                              |     |     |     |     |
| cpe:2.3:a:fedoraproject:389_directory_server:****:*:*:     |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux:7.0:****:*:*:            |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux:7.0:****:*:*:            |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:****:*:*:    |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:****:*:*:    |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server:7.0:****:*:*:     |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server:7.0:****:*:*:     |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:****:*:*: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:****:*:*: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:****:*:*: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:****:*:*: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:****:*:*: |        |                              |     |     |     |     |
| cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:****:*:*: |        |                              |     |     |     |     |

|                                                              |
|--------------------------------------------------------------|
| cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*:*:*:*:*:  |
| cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*: |
| cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*: |

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→