



# CVE-2021-4091

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-4091   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-02-18 18:15:00 UTC   |
| <b>Updated</b>         | 2023-04-24 09:15:00 UTC   |
| <b>Description</b>     | A double-free was found in the way 389-ds-base handles virtual attributes context in persistent searches. An attacker could |

## Risk And Classification

**Problem Types:** CWE-415

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor  | Product                                   | Version | Update | Edition | Language |
|------------------|---------|---|---------|--------|---------|----------|
| Application      | Port389 | 389-ds-base                               | All     | All    | All     | All      |
| Operating System | Redhat  | Enterprise Linux Desktop                  | 7       | All    | All     | All      |
| Operating System | Redhat  | Enterprise Linux For Ibm Z Systems        | 7.0     | All    | All     | All      |
| Operating System | Redhat  | Enterprise Linux For Power Big Endian     | 7.0     | All    | All     | All      |
| Operating System | Redhat  | Enterprise Linux For Power Little Endian  | 7.0     | All    | All     | All      |
| Operating System | Redhat  | Enterprise Linux For Scientific Computing | 7.0     | All    | All     | All      |
| Operating System | Redhat  | Enterprise Linux Server                   | 7.0     | All    | All     | All      |
| Operating System | Redhat  | Enterprise Linux Workstation              | 7.0     | All    | All     | All      |

## References

| Reference  | Source  | Link                  |
|--|---------|-----------------------|
| [SECURITY] [DLA 3399-1] 389-ds-base security update  | MLIST   | <a href="#">lists</a> |
| 2030307 – (CVE-2021-4091) CVE-2021-4091 389-ds-base: double-free of the virtual attribute context in persistent search | MISC    | <a href="#">bug:</a>  |
| CVE Program record   | CVE.ORG | <a href="#">www</a>   |
| NVD vulnerability detail   | NVD     | <a href="#">nvd.</a>  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159675](#) Oracle Enterprise Linux Security Update for 389-ds-base security and bug fix update (ELSA-2022-0628)

[159710](#) Oracle Enterprise Linux Security Update for 389-ds:1.4 (ELSA-2022-0889)

[181751](#) Debian Security Update for 389-ds-base (DLA 3399-1)

[183241](#) Debian Security Update for 389-ds-base (CVE-2021-4091)

[240103](#) Red Hat Update for 389-ds-base (RHSA-2022:0628)

[240153](#) Red Hat Update for 389-ds:1.4 (RHSA-2022:0889)

[240219](#) Red Hat Update for 389-ds:1.4 (RHSA-2022:1410)

[257158](#) CentOS Security Update for 389-ds-base (CESA-2022:0628)

[353990](#) Amazon Linux Security Advisory for 389-ds-base : ALAS2-2022-1819

[354046](#) Amazon Linux Security Advisory for 389-ds-base : ALAS-2022-1629

[377264](#) Alibaba Cloud Linux Security Update for 389-ds-base (ALINUX2-SA-2022:0012)

[377398](#) Alibaba Cloud Linux Security Update for 389-ds:1.4 (ALINUX3-SA-2022:0020)

[752244](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:2109-1)

[752245](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:2105-1)

[752257](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:2163-1)

[753164](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:2295-1)

[753336](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:2081-1)

[940467](#) AlmaLinux Security Update for 389-ds:1.4 (ALSA-2022:0889)

[960742](#) Rocky Linux Security Update for 389-ds:1.4 (RLSA-2022:0889)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)