



# CVE-2022-0996

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

## Summary

<b>CVE</b>	CVE-2022-0996
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-23 20:15:00 UTC
<b>Updated</b>	2023-08-08 14:21:00 UTC
<b>Description</b>	A vulnerability was found in the 389 Directory Server that allows expired passwords to access the database to cause improv

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">389 Directory Server</a>	1.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">389 Directory Server</a>	1.4.0.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
[SECURITY] Fedora 34 Update: 389-ds-base-2.0.15-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fec</a>
GitHub - ByteHackr/389-ds-base	MISC	<a href="#">github.</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
2064769 – (CVE-2022-0996) CVE-2022-0996 389-ds-base: expired password was still allowed to access the database	MISC	<a href="#">bugzill</a>
[SECURITY] [DLA 3399-1] 389-ds-base security update	MISC	<a href="#">lists.de</a>
[SECURITY] Fedora 35 Update: 389-ds-base-2.0.15-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fec</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>

[SECURITY] Fedora 34 Update: 389-ds-base-2.0.15-1.fc34 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fec</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
[SECURITY] Fedora 35 Update: 389-ds-base-2.0.15-1.fc35 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fec</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159917](#) Oracle Enterprise Linux Security Update for 389-ds-base (ELSA-2022-5239)

[160018](#) Oracle Enterprise Linux Security Update for 389-ds:1.4 (ELSA-2022-5823)

[160301](#) Oracle Enterprise Linux Security Update for 389-ds-base (ELSA-2022-8162)

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

[184849](#) Debian Security Update for 389-ds-base (CVE-2022-0996)

[240493](#) Red Hat Update for 389-ds-base security (RHSA-2022:5239)

[240551](#) Red Hat Update for 389-ds:1.4 (RHSA-2022:5620)

[240582](#) Red Hat Update for 389-ds:1.4 (RHSA-2022:5823)

[240906](#) Red Hat Update for 389-ds-base security (RHSA-2022:8162)

[241011](#) Red Hat Update for 389-ds-base (RHSA-2022:8976)

[257183](#) CentOS Security Update for 389-ds-base (CESA-2022:5239)

[282545](#) Fedora Security Update for 389 (FEDORA-2022-40544b5314)

[282546](#) Fedora Security Update for 389 (FEDORA-2022-2558f14c58)

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

[377303](#) Alibaba Cloud Linux Security Update for 389-ds-base (ALINUX2-SA-2022:0029)

[377555](#) Alibaba Cloud Linux Security Update for 389-ds:1.4 (ALINUX3-SA-2022:0156)

[671702](#) EulerOS Security Update for 389-ds-base (EulerOS-SA-2022-1701)

[671857](#) EulerOS Security Update for 389-ds-base (EulerOS-SA-2022-1881)

[671887](#) EulerOS Security Update for 389-ds-base (EulerOS-SA-2022-1921)

[751965](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:1102-1)

[751966](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:1102-1)

<a href="#">751968</a> OpenSUSE Security Update for 389-ds (openSUSE-SU-2022:1100-1)
<a href="#">751977</a> SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:1139-1)
<a href="#">752257</a> SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:2163-1)
<a href="#">753446</a> SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:1100-1)
<a href="#">940605</a> AlmaLinux Security Update for 389-ds:1.4 (ALSA-2022:5823)
<a href="#">940813</a> AlmaLinux Security Update for 389-ds-base (ALSA-2022:8162)
<a href="#">960294</a> Rocky Linux Security Update for 389-ds:1.4 (RLSA-2022:5823)
<a href="#">960625</a> Rocky Linux Security Update for 389-ds-base (RLSA-2022:8162)

© [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](#)**