



CVE-2022-2850

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

Summary

CVE	CVE-2022-2850
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-14 18:15:00 UTC
Updated	2023-05-18 18:04:00 UTC
Description	A flaw was found in 389-ds-base. When the Content Synchronization plugin is enabled, an authenticated user can reach a

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Port389	389-ds-base	All	All	All	All
Operating System	Redhat	389 Directory Server	All	All	All	All
Application	Redhat	Directory Server	11.0	All	All	All
Application	Redhat	Directory Server	12.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	

2118691 – (CVE-2022-2850) CVE-2022-2850 389-ds-base: SIGSEGV in sync_repl	MISC	bugzilla.redhat.com	
[SECURITY] [DLA 3399-1] 389-ds-base security update	MISC	lists.debian.org	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160166](#) Oracle Enterprise Linux Security Update for 389-ds-base (ELSA-2022-7087)

[160185](#) Oracle Enterprise Linux Security Update for 389-ds:1.4 (ELSA-2022-7133)

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

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

[182319](#) Debian Security Update for 389-ds-base (CVE-2022-2850)

[240775](#) Red Hat Update for 389-ds:1.4 (RHSA-2022:7133)

[240777](#) Red Hat Update for 389-ds-base (RHSA-2022:7087)

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

[240952](#) Red Hat Update for 389-ds:1.4 (RHSA-2022:8680)

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

[257197](#) CentOS Security Update for 389-ds-base (CESA-2022:7087)

[354138](#) Amazon Linux Security Advisory for 389-ds-base : ALAS2-2022-1879

[377743](#) Alibaba Cloud Linux Security Update for 389-ds-base (ALINUX2-SA-2022:0051)

[377747](#) Alibaba Cloud Linux Security Update for 389-ds:1.4 (ALINUX3-SA-2022:0178)

[672137](#) EulerOS Security Update for 389-ds-base (EulerOS-SA-2022-2437)

[753398](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:3029-1)

[753463](#) SUSE Enterprise Linux Security Update for 389-ds (SUSE-SU-2022:3286-1)

[940720](#) AlmaLinux Security Update for 389-ds:1.4 (ALSA-2022:7133)

[940813](#) AlmaLinux Security Update for 389-ds-base (ALSA-2022:8162)

[960192](#) Rocky Linux Security Update for 389-ds:1.4 (RLSA-2022:7133)

[960625](#) 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](#)