CVE-2022-2850

Public on August 3, 2022
Last Modified: November 15, 2022 at 1:23:14 PM UTC

MODERATE

Moderate Impact
What does this mean?

6.5

CVSS v3 Base Score
CVSS Score Breakdown

Insights vulnerability analysis

View exposed systems →

Description

A flaw was found In 389-ds-base. When the Content Synchronization plugin is enabled, an authenticated user can reach a NULL pointer dereference using a specially crafted query. This flaw allows an authenticated attacker to cause a denial of service.

Statement

This CVE is assigned against an incomplete fix of CVE-2021-3514.

Additional Information

- Bugzilla 2118691: CVE-2022-2850 389-ds-base: SIGSEGV in sync_repl
- CWE-476: NULL Pointer Dereference
- FAQ: Frequently asked questions about CVE-2022-2850

Affected Packages and Issued Red Hat Security Errata

Platform	Package	State	Errata	Release Date
Red Hat Directory Server 12	redhat-ds:12/389-ds-base	Affected		
Red Hat Directory Server 11	redhat-ds:11/389-ds-base	Affected		
Red Hat Enterprise Linux 8	389-ds:1.4	Fixed	RHSA-2022:7133	October 25, 2022
Red Hat Enterprise Linux 6	389-ds-base	Out of support scope		
Red Hat Enterprise Linux 7	389-ds-base	Fixed	RHSA-2022:7087	October 25, 2022
Red Hat Enterprise Linux 9	389-ds-base	Fixed	RHSA-2022:8162	November 15, 2022

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	6.5	6.5
Attack Vector	Network	Network
Attack Complexity	Low	Low
Privileges Required	Low	Low
User Interaction	None	None
Scope	Unchanged	Unchanged
Confidentiality	None	None
Integrity Impact	None	None
Availability Impact	High	High

CVSS v3 Vector

Red Hat:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
NVD:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Acknowledgements

This issue was discovered by Viktor Ashirov (Red Hat).

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors? ›

My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability? ›

What can I do if my product is listed as "Will not fix"? ›

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected? ›

My product is listed as "Out of Support Scope". What does this mean? ›

Not sure what something means? Check out our Security Glossary.

This page is generated automatically and has not been checked for errors or omissions.
For clarification or corrections please contact Red Hat Product Security.

Last Modified: November 15, 2022 at 1:23:14 PM UTC