Bug 2118691 (CVE-2022-2850) - CVE-2022-2850 389-ds-base: SIGSEGV in sync_repl

Keywords: Security ×

Status: NEW

Alias: CVE-2022-2850

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2118761 2118762 2119110 2131744 2134136 2136307 2118763 2118764 2118765 2119109 2131083 2131743 2134816

Blocks: 2115680

TreeView+ depends on / blocked

Reported: 2022-08-16 13:18 UTC by Sandipan Roy

Modified: 2022-11-15 12:41 UTC (History)

CC List: 8 users (show)

Fixed In Version:

Doc Type: If docs needed, set a value

Doc Text: 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.

Clone Of:

Environment:

Last Closed:

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2022:7087	0	None	None	None	2022-10-25 07:44:50 UTC
Red Hat Product Errata	RHSA-2022:7133	0	None	None	None	2022-10-25 09:35:22 UTC
Red	RHSA-	0	None	None	None	2022-

Hat Product Errata	2022:8162					11-15 10:30:13 UTC

Sandipan Roy 2022-08-16 13:18:35 UTC Description

```
Description of problem:
Previously: https://bugzilla.redhat.com/show_bug.cgi?
id=1952907

This issue is not fixed completely and can be triggered by
supplying a malformed cookie, for example -E sync=rp/foo

Thread 14 "ns-slapd" received signal SIGSEGV, Segmentation
fault.
0x00007f7802ba38d6 in __strcmp_evex () from
target:/lib64/libc.so.6
(gdb) bt
#0  0x00007f7802ba38d6 in __strcmp_evex () at
target:/lib64/libc.so.6
#1  0x00007f77fe926e9f in sync_cookie_isvalid
(refcookie=0x7f77febfaba0, testcookie=0x7f77febfab80)
    at ldap/servers/plugins/sync/sync_util.c:796
#2  sync_cookie_isvalid (testcookie=0x7f77febfab80,
refcookie=0x7f77febfaba0) at
ldap/servers/plugins/sync/sync_util.c:789
#3  0x00007f77fe92aa7d in sync_srch_refresh_pre_search
(pb=0x7f77feb9fd00) at
ldap/servers/plugins/sync/sync_refresh.c:135
#4  0x00007f7802e297d9 in plugin_call_func
    (list=0x7f77fe9ed800, operation=operation@entry=403,
pb=pb@entry=0x7f77feb9fd00, call_one=call_one@entry=0)
    at ldap/servers/slapd/plugin.c:2001
#5  0x00007f7802e299e6 in plugin_call_list (pb=0x7f77feb9fd00,
operation=403, list=<optimized out>) at
ldap/servers/slapd/plugin.c:1944
#6  plugin_call_plugins (pb=0x7f77feb9fd00, whichfunction=403)
at ldap/servers/slapd/plugin.c:414
#7  0x00007f7802e222a9 in op_shared_search
(pb=pb@entry=0x7f77feb9fd00, send_result=send_result@entry=1)
at ldap/servers/slapd/opshared.c:586
#8  0x0000556eb3f0db14 in do_search (pb=<optimized out>) at
ldap/servers/slapd/search.c:388
#9  0x0000556eb3efcb7f in connection_dispatch_operation
(pb=0x7f77feb9fd00, op=<optimized out>, conn=<optimized out>)
    at ldap/servers/slapd/connection.c:659
#10 connection_threadmain () at
ldap/servers/slapd/connection.c:1785
#11 0x00007f780290ec34 in _pt_root () at
target:/lib64/libnspr4.so
#12 0x00007f7802b75802 in start_thread () at
target:/lib64/libc.so.6
#13 0x00007f7802b15450 in clone3 () at target:/lib64/libc.so.6


Automated reproducer: https://github.com/389ds/389-ds-
base/blob/main/dirsrvtests/tests/tickets/ticket48013_test.py

Version-Release number of selected component (if applicable):
389-ds-base-2.0.x+ (earliest I was able to test was 2.0.5).

How reproducible:
Deterministically
```

Steps to Reproduce:
1. https://github.com/389ds/389-ds-base/blob/main/dirsrvtests/tests/tickets/ticket48013_test.py

Actual results:
Server crashes

Expected results:
Should return an error that the cookie is invalid and not crash.

Additional info:
Upstream ticket: https://github.com/389ds/389-ds-base/issues/4711#issuecomment-1205100979

Sandipan Roy 2022-08-16 17:11:48 UTC Comment 1

Created 389-ds-base tracking bugs for this issue:

Affects: fedora-35 [bug 2118761]
Affects: fedora-36 [bug 2118762]

errata-xmlrpc 2022-10-25 07:44:48 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 7

Via RHSA-2022:7087 https://access.redhat.com/errata/RHSA-2022:7087

errata-xmlrpc 2022-10-25 09:35:19 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2022:7133 https://access.redhat.com/errata/RHSA-2022:7133

errata-xmlrpc 2022-11-15 10:30:11 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2022:8162 https://access.redhat.com/errata/RHSA-2022:8162

Note

You need to log in before you can comment on or make changes to this bug.