Status: VERIFIED FIXED

Product: OpenLDAP
Component: slapd (show other issues)

Version: unspecified Hardware: All All

Importance: --- normal Target Milestone: 2.5.1

Assignee: OpenLDAP project

URL:

Depends on:

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

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

```
2021-02-06 09:06:05 UTC
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Description
            A malicious packet can force OpenLDAP to fail an assertion and crash slapd: schema_init.c:3808: checkTime: Assertion `!BER_EVISEMPTY( in )' failed.
Output:

(Interpretation of the state of the
                                Goldede get filter: unknown filter type=48
Slapdi schem filter junknown filter type=48
Slapdi schem filter: unknown filter: unknow
                                seting:
Launch openIdap
(Current public repo)
docker run it -netHoost bitnami/openIdap
docker run -it -netHoost bitnami/openIdap
docker run -it -netHoost phasip/openIdap
2. Bend crashing packet
kal 0.823/u01iksing packet
no localhost 150/u01iksing 2020ket
```

-- Note -I had forgotten the fuzzer was running. As only one crash has been found in a while the fuzzing machine will retire now. I will collect the corpus into https://dithub.com/Phasio/popenlagh fuzz

fixed in master

Comment 1 Comment 2

Ouanah Gibson-Mount 2021-02-06 22:21:10 UTC

• 3539fc33 by Howard Chu at 2021-02-06T20:52:06+00:00 ITS#9454 fix issuerAndThisUpdateCheck

- wzacurc/
by Howard Chu at 2021-02-06T22:09:40+00:00
ITS#9454 fix issuerAndThisUpdateCheck

RE24:

by Howard Chu at 2021-02-06T22:19:57+00:00 ITS#9454 fix issuerAndThisUpdateCheck

Reported: 2021-02-06 09:06 UTC by phasip Modified: 2021-09-11 10:11 UTC (<u>History</u>) CC List: 0 users

See Also: