

DoS and code execution issue in LedgerSMB < 1.1.5 and SQL-Ledger < 2.6.25

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-03/msg00058.html>

- *From:* Chris Travers <chris@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 05 Mar 2007 11:43:36 -0800
-

Hi;

A person on the LedgerSMB core team has found a serious arbitrary code execution issue in LedgerSMB prior to 1.1.5 and SQL-Ledger. A version of SQL-Ledger which fixes this vulnerability was released today (version 2.6.25).

The vulnerability allows a user to specify a custom function to run when the software encounters an error. The software further assumes that the error function specified never returns. For this reason, it is possible to cause the software to take alternate paths of execution, and to force these paths. This is particularly dangerous for users with valid logins.

For those which do not have valid login credentials, the problem more limited but still quite dangerous. Using this method it is possible to overwrite files in the users directory, thus affecting a DoS attack and possible authentication bypass.

The DoS attacks can be done by any user not currently logged in, and can force the writing of a nologin file (which will lock users out of the system) or overwrite the users/members file (which contains users' credentials info and settings) with invalid data. This attack can be done with wget, for example.

All SQL-Ledger users are advised to upgrade to the latest version, and all LedgerSMB users using versions prior to 1.1.5 should upgrade as well.

Best Wishes,
Chris Travers
begin:vcard
fn:Chris Travers
n:Travers;Chris
email;internet:chris@xxxxxxxxxxxxxxxxxxx
tel;work:509-888-0220
tel;cell:509-630-7794
x-mozilla-html:FALSE
version:2.1
end:vcard