

Full disclosure: Directory Transversal and Arbitrary Code Execution Vulnerability in SQL-Ledger and LedgerSMB

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-03/msg00001.html>

- *From:* Chris Travers <chris@xxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 28 Feb 2007 17:26:55 -0800
-

Hi all;

Another security issue has been found in LedgerSMB < 1.1.5 and all versions of SQL-Ledger which allows an attacker to engage in directory transversal, retrieval of sensitive information, user account fabrication, or even arbitrary code execution. This was fixed in LedgerSMB 1.1.5 and despite ample warning, the maintainer of SQL-Ledger has not corrected the problem.

The problem occurs because the blacklisting functions for the text editor strip out potentially dangerous targets rather than denying access when a problem is detected. The stripping of such "dangerous" elements involves first stripping the \$userpath (usually users) and then the \$memberfile (by default users/members) and then opening the file that remains.

So, to go up two levels and open foo.txt, you could pass a url containing the argument of file=.users./users/members./foo.txt to the url for editing the template. After these are stripped out, you are left with ../../foo.txt. You can also retrieve the memberfile by using the path of file=useuserusers/memberssrs/members. Then by crafting a similar URL or by altering the web page to post custom variables, you can cause the application to overwrite this file, possibly deleting or changing passwords, or adding user accounts.

This can also be used to cause arbitrary code to be executed as well. SQL-Ledger and LedgerSMB < 1.2 rely on server-writable and executable Perl scripts to store user preferences. These scripts are run at every page load, are created on login, and destroyed at logout. Using the same method, you can add arbitrary Perl code to the end of these files causing that to be loaded the next time the target user loads a page.

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