



CVE-2021-3882

Published on: 10/14/2021 12:00:00 AM UTC

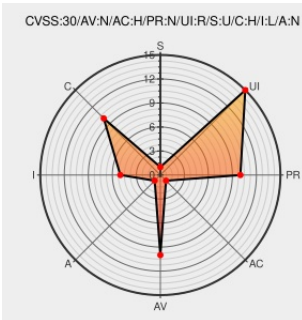
Last Modified on: 10/20/2021 06:02:00 PM UTC

CVE-2021-3882 - advisory for 7061d97a-98a5-495a-8ba0-3a4c66091e9d

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



Certain versions of [Ledgersmb](#) from [Ledgersmb](#) contain the following vulnerability:

LedgerSMB does not set the 'Secure' attribute on the session authorization cookie when the client uses HTTPS and the LedgerSMB server is behind a reverse proxy. By tricking a user to use an unencrypted connection (HTTP), an attacker may be able to obtain the authentication data by capturing network traffic. LedgerSMB 1.8 and

newer switched from Basic authentication to using cookie authentication with encrypted cookies. Although an attacker can't access the information inside the cookie, nor the password of the user, possession of the cookie is enough to access the application as the user from which the cookie has been obtained. In order for the attacker to obtain the cookie, first of all the server must be configured to respond to unencrypted requests, the attacker must be suitably positioned to eavesdrop on the network traffic between the client and the server *and* the user must be tricked into using unencrypted HTTP traffic. Proper audit control and separation of duties limit Integrity impact of the attack vector. Users of LedgerSMB 1.8 are urged to upgrade to known-fixed versions. Users of LedgerSMB 1.7 or 1.9 are unaffected by this vulnerability and don't need to take action. As a workaround, users may configure their Apache or Nginx reverse proxy to add the Secure attribute at the network boundary instead of relying on LedgerSMB. For Apache, please refer to the 'Header always edit' configuration command in the mod_headers module. For Nginx, please refer to the 'proxy_cookie_flags' configuration command.

CVE-2021-3882 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **ledgersmb** - ledgersmb/ledgersmb version >= 1.8.0

Affected Vendor/Software: **ledgersmb** - ledgersmb/ledgersmb version <= 1.8.21

CVSS3 Score: **6.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED

NETWORK	HIGH	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	NONE
CVSS2 Score: 4 - MEDIUM			
Access Vector	Access Complexity	Authentication	
NETWORK	HIGH	NONE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	PARTIAL	NONE	

CVE References

Description	Tags	Link
Page not found LedgerSMB	ledgersmb.org text/html Inactive Link Not Archived	MISC ledgersmb.org/cve-2021-3882-sensitive-non-secure-cookie
Use HTTPS environment setting to detect https connections · ledgersmb/LedgerSMB@c242f5a · GitHub	github.com text/html	MISC github.com/ledgersmb/ledgersmb/commit/c242f5a2abf4b99b0da205473cbb...
huntr: Disclose & Fix Security Vulnerabilities in Open Source	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/7061d97a-98a5-495a-8ba0-3a4c66091e9d

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ledgersmb	Ledgersmb	1.8.0	-	All	All
cpe:2.3:a:ledgersmb:ledgersmb:1.8.0:-:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3882 : LedgerSMB does not set the 'Secure' attribute on the session authorization cookie when the client u... twitter.com/i/web/status/1...	2021-10-14 08:24:44

© CVE.report 2021   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)