Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in ledgersmb/ledgersmb

0

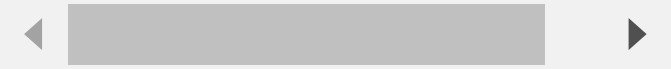
Valid Reported on Sep 15th 2021

Description

Secure flag is not implemented on the application

Proof of Concept

```
https://drive.google.com/file/d/1ESnBKwFef8D42A2VD3W59vXMLdWhCxS9/view?usp=
```



Impact

The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. To accomplish this goal, browsers which support the secure flag will only send cookies with the secure flag when the request is going to a HTTPS page. Said in another way, the browser will not send a cookie with the secure flag set over an unencrypted HTTP request. By setting the secure flag, the browser will prevent the transmission of a cookie over an unencrypted channel.

References

- https://portswigger.net/kb/issues/00500200_tls-cookie-without-secure-flag-set

CVE
CVE-2021-3882
(Published)

Vulnerability Type
CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Severity
Medium (5.9)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

0xdhinu
@0xdhinu
unranked

This report was seen 627 times.

We have contacted a member of the **ledgersmb** team and are waiting to hear back a year ago

A **ledgersmb/ledgersmb** maintainer a year ago — Maintainer

Although you tested this with an unsupported version (superseded by newer releases) and I'd like to argue that this is a mis-configuration on the site you're reporting this on (which it is), I'm currently researching what's required on newer versions to do correct configuration and whether the project distributes example configuration which supports this scenario out of the box.

A **ledgersmb/ledgersmb** maintainer a year ago — Maintainer

This report is valid. It does however, strictly concern 1.8.x versions: all earlier versions don't store secret data in the session cookie as the cookie only contains a "session verification" token (csrf-like), but not the session authorization itself.

@admin, could you set the CVSS score to 5.9? The CVSS3.1 vector outcome of our assessment is CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N .

A **ledgersmb/ledgersmb** maintainer validated this vulnerability a year ago

0xdhinu has been awarded the disclosure bounty ✅

The fix bounty is now up for grabs

A **ledgersmb/ledgersmb** maintainer a year ago Maintainer

@admin, please allocate a CVE number; we have a fix ready for release.

Jamie Slome a year ago Admin

@maintainer - CVE assigned! 🎊

Can you please confirm the fix commit SHA + the fixed version?

@0xdhinu - can you please update the CVSS to the vector provided by the maintainer above?

Jamie Slome marked this as fixed with commit **c242f5** a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Jamie Slome a year ago Admin

CVE published! 🎊

Sign in to join this conversation