[CVE-2020-16093] Peer certificate not checked when using LDAPS

Environment

LemonLDAP::NG version: 2.0.8

Operating system: Debian 10

Summary

- Configure a `ldaps://` URL as `ldapServer`
- Setup a self signed certificate on the LDAP server
- It works
- (It should not work.)

Possible fixes

Net::LDAP is insecure by default, at least on Debian Buster. We should explicitely pass `verify => require` when initializing it.

Fixing this is probably going to break a lot of installs. We need to create a new option for this and add a warning to release notes.

Edited 2 years ago by Maxime Besson

⬆ Drag your designs here or click to upload.

Tasks ⊙ 0	
No tasks are currently assigned. Use tasks to break down this issue into smaller parts.	

Linked items ⊘ 0	
Link issues together to show that they're related. Learn more.	

Activity

🕐 **Maxime Besson** changed milestone to %2.0.9 2 years ago

🏷 **Maxime Besson** added Bug Portal Security labels 2 years ago

✎ **Maxime Besson** changed the description 2 years ago

Maxime Besson @maxbes · 2 years ago — Author | Maintainer
https://rt.cpan.org/Ticket/Display.html?id=131045

Maxime Besson @maxbes · 2 years ago — Author | Maintainer

It seems to me like improper validation of remote certificates deserves a CVE, and that the default setting should be to validate. But it will break stuff for many users who setup ldaps:// connection without caring properly about certificate authorities.

what do you think @guimard ?

Clément OUDOT @clement_oudot · 2 years ago — Owner

Yes, a CVE should be opened. And we should allow an option to disable the verification, but the default behavior has to be changed as you suggest. Ok @guimard ?

✎ **Maxime Besson** changed title from **Peer certificate not checked when using LDAPS** to **[CVE-2020-16093] Peer certificate not checked when using LDAPS** 2 years ago

---

Maxime Besson @maxbes · 2 years ago — Author | Maintainer

This bug has been assigned CVE number CVE-2020-16093

Edited by Maxime Besson 2 years ago

Clément OUDOT @clement_oudot · 2 years ago — Owner

Fix will be commited just before release. The default behavior will be to check certificate. An option will allow to bypass the check. An uograde note will be written.

💬 **Maxime Besson** mentioned in commit 4e5578e3 2 years ago

💬 **Maxime Besson** mentioned in commit 3771ead3 2 years ago

💬 **Maxime Besson** mentioned in commit c6358d75 2 years ago

💬 **Maxime Besson** mentioned in commit 36a1b1c8 2 years ago

💬 **Maxime Besson** mentioned in commit fde469b0 2 years ago

Maxime Besson @maxbes · 2 years ago — Author | Maintainer

Tested:

- CentOS7, Debian Buster
- ldaps://, ldap+tls://, ldap:// with or without cert validation, with or without a valid certificate

TODO:

- update Apache::Session(::Browseable)?::LDAP with the CentOS workaround (see https://gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/blob/3771ead3dba5ae67fc8fe0011d78a0e0a42c7361/lemonldap-ng-portal/lib/Lemonldap/NG/Portal/Lib/Net/LDAP.pm#L65)
- add a comment in release notes to remind users to update their LDAP session module if they want to enable certificate validation

Edited by Maxime Besson 2 years ago

Clément OUDOT @clement_oudot · 2 years ago — Owner

Hello @xavierb

we push on CPAN today new releases for Apache::Session::LDAP and Apache::Session::Browseable. They will be published on our yum repository but should also be quickly updated on EPEL. If you can help on this it would be great.

👁 **Clément OUDOT** made the issue visible to everyone 2 years ago

💬 **Clément OUDOT** mentioned in commit 9306674c 2 years ago

⊖ **Clément OUDOT** closed 2 years ago

Yadd @guimard · 2 years ago — Owner

Hi; here we should have pushed 1 CVE for each software (+ Apache::Session::LDAP and Apache::Session::Browseable). Not important since issue can be considered as minor

---

Please register or sign in to reply