

Redmine - Defect #29476

Update net-ldap to 0.16.0

2018-09-02 11:57 - Yuuki NARA

Status: Closed	Start date:
Priority: Normal	Due date:
Assignee:	% Done: 0%
Category: Gems support	Estimated time: 0.00 hour
Target version:	Affected version: 3.4.6
Resolution: Wont fix	

Description

Redmine 3.4-stable specifies net-ldap 0.12.0 in Gemfile.

There is a known vulnerability, and an update to 0.16.0 is recommended. (CVE-2017-17718)

Redmine trunk has already been updated to 0.16.0.
#24970

Please also implement the same fix for 3.4-stable.

In Github's repository, vulnerabilities are being warned.

CVE-2017-17718
The Net::LDAP (aka net-ldap) gem before 0.16.0 for Ruby has Missing SSL Certificate Validation.

Gemfile update suggested:
net-ldap ~> 0.16.0

Related issues:

Related to Redmine - Defect # 24970: Net::LDAP::LdapError is deprecated	Closed
Related to Redmine - Patch # 29606: Support self-signed LDAPS connections	Closed

History

#1 - 2018-09-02 12:11 - Yuuki NARA

- File *github-netldap-warning.png* added

Github vulnerability warning screen.

github-netldap-warning.png

#2 - 2018-09-02 17:54 - Marius BALTEANU

- Description updated

#3 - 2018-09-02 17:55 - Marius BALTEANU

- Related to Defect #24970: Net::LDAP::LdapError is deprecated added

#4 - 2018-09-13 15:58 - Holger Just

- Related to Patch #29606: Support self-signed LDAPS connections added

#5 - 2018-09-14 07:13 - Go MAEDA

- *Category set to Gems support*

According to #29606, net-ldap 0.16.0 rejects self-signed certificates by default. It may affect some on-premise installations if we upgrade net-ldap without implementing #29606.

However, in my opinion, the patch #29606 should not be merged into 3.4-stable/3.3-stable branches because it has a database migration.

#6 - 2018-12-18 01:13 - Go MAEDA

- *Status changed from New to Closed*

- *Resolution set to Wont fix*

I think we should not update the gem in 3.4-stable branch because there is a compatibility problem I wrote in #29476#note-5. In the worst case, users cannot log in after upgrading.

I recommend upgrading to Redmine 4.0.0 if the vulnerability matters.

Files

github-netldap-warning.png	157 KB	2018-09-02	Yuuki NARA
----------------------------	--------	------------	------------