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:			
Resolution:	Wont fix	**Affected version:**	3.4.6

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:

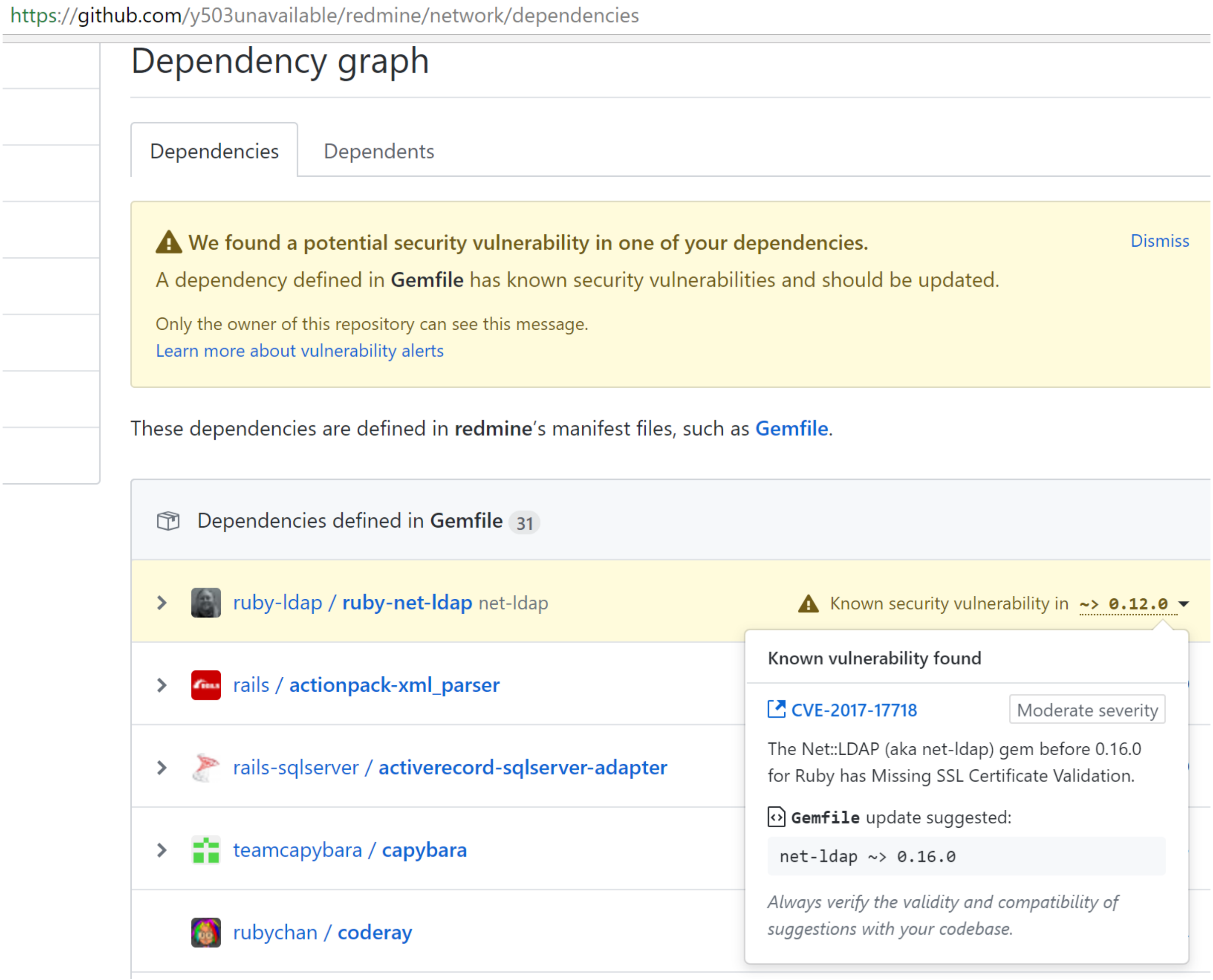
Related to Redmine - Defect #24970: Net::LDAP::LdapError is deprecated	**Closed**
Related to Redmine - Patch #29606: Support self-signed LDAPS connections	**Closed**

History

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

- File github-netldap-warning.png added

Github vulnerability warning secreen.



https://github.com/y503unavailable/redmine/network/dependencies

Dependency graph

Dependencies | Dependents

We found a potential security vulnerability in one of your dependencies. Dismiss

A dependency defined in **Gemfile** has known security vulnerabilities and should be updated.

Only the owner of this repository can see this message.
Learn more about vulnerability alerts

These dependencies are defined in **redmine**'s manifest files, such as **Gemfile**.

Dependencies defined in **Gemfile** 31

- ruby-ldap / **ruby-net-ldap** net-ldap — Known security vulnerability in `~> 0.12.0`
- rails / **actionpack-xml_parser**
- rails-sqlserver / **activerecord-sqlserver-adapter**
- teamcapybara / **capybara**
- rubychan / **coderay**

Known vulnerability found

CVE-2017-17718 — Moderate severity

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
```

Always verify the validity and compatibility of suggestions with your codebase.

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

- Description updated

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

- 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