New issue

Jump to bottom

Security: SSL/TLS certificate validation for LDAP disabled by default #3482

Closed **robert-scheck** opened this issue on Jan 25, 2021 · 5 comments

robert-scheck commented on Jan 25, 2021 Contributor

As of writing, Wekan disables the SSL/TLS certificate validation for LDAP by default unless `LDAP_REJECT_UNAUTHORIZED=true` is explicitly set. Thus, by default, Wekan is effectively vulnerable to MITM attacks, even when using SSL/TLS for LDAP. I treat this default behaviour as bad, given that security shouldn't be opt-in but opt-out (e.g. for test-only environments). As this behaviour does not seem to be properly documented for system administrators (at least not outside of the source code), I would treat this as a vulnerability following CWE-295: Improper Certificate Validation and thus as a CVE-worthy candidate.

Oh, and please note that Node.js itself has, according to its documentation, a security-wise default by having `true` as default for `rejectUnauthorized`.

robert-scheck added a commit to robert-scheck/wekan that referenced this issue on Jan 25, 2021

`Reject by default LDAP connections not authorized via CA trust store ...` 31f8912

This was referenced on Jan 25, 2021

Reject by default LDAP connections not authorized via CA trust store #3483

Merged

Unable to pass trusted root CA certificate via LDAP_CA_CERT #3484

Closed

xet7 commented on Jan 25, 2021 Member

Fixed at #3483

xet7 closed this as completed on Jan 25, 2021

robert-scheck commented on Jan 25, 2021 Contributor Author

Wow, thank you for the quick review and merge!

robert-scheck commented on Jan 26, 2021 Contributor Author

CVE-2021-3309 was assigned by MITRE a few minutes ago.

robert-scheck mentioned this issue on Jan 28, 2021

LDAP login failure with 4.87.0 #3493

Closed

xet7 commented on Feb 2, 2021 Member

@robert-scheck

And also a few minutes ago, added to CVE Hall of Fame https://wekan.github.io/hall-of-fame/

xet7 commented on Feb 2, 2021 Member

@robert-scheck

Thanks for helping with getting CVE numbers! I have not yet got CVE numbers for all of those at Wekan CVE HoF.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants