GitBITS

By GitLab Security

Topic: GitLab Self-Managed Security Hardening

One of the most common questions for self-managed customers is *how can I properly harden my GitLab standalone instance?* As these customers do not leverage the native security configurations offered to SaaS customers, they have to enforce additional security controls themselves. That is why we created the Security Hardening Guide for Self-Managed.

Mark Loveless from the Security Research team went through all of the available features, configurations and controls available to self-managed customers. For each, he determined the settings that would secure the installation the most.

Five main sections are included in this guide:

1. General Hardening Concepts
2. Åpplication Recommendations
3. CI/CD Recommendations
4. Configuration Recommendations
5. Operating System Recommendations

The objective is for customers to install a GitLab instance that is as secure as it can be. The hardening process involves turning off unused features, making adjustments to settings that have security implications, and generally trying to limit the overall exposure of data as much as possible while still allowing the underlying applications to run.

The guide is available on the GitLab security documentation and the key hardening measures are highlighted in the blog post: How to harden your self-managed GitLab instance. Updates were made to numerous documentation entries as part of this effort. Please review our secure your installation page for the list of security measures to keep in mind.

To learn more about Security at GitLab, see our handbook page.

Visit our Trust Center to learn more about GitLab Security!