Security

The security of Stiltsoft Europe ("Stiltsoft Europe", "we" or "our") customers' data is our highest priority, and we follow the best practices to keep your data safe.

Overview

TeamCity Integration for Jira app (the “App”) is part of the Bug Bounty Program, which helps detect security vulnerabilities faster and increase the overall security level for our customers.

Our cloud security strategy is based on the CSA Cloud Controls Matrix (CCM). We also use CAIQ-Lite as a baseline mechanism to express our security posture and to provide security control transparency. The completed CAIQ-Lite questionnaire can be obtained upon request in our support system via the Whistic platform.

If you have questions or feedback regarding security with TeamCity Integration for Jira or would like to report a security vulnerability, please send an email to tech-support@stiltsoft.com or create a request in the support system.

Secure development

We follow the best practices and frameworks to ensure the highest level of security in our software:

- Regular security trainings for developers to learn about common vulnerabilities and threats
- Code review for security vulnerabilities
- Regular update of the dependencies
- Static Application Security Testing (SAST) to detect vulnerabilities in our codebase
- Software Composition Analysis (SCA) tools to keep track of open source components used by your applications

Employee Access to Customer Data

The App’s team does not have access to user data. Our employees connect to the infrastructure via secure communication channels with several levels of protection.

Working on a support issue we only access the minimum data needed to resolve the issue.

Product Security

Users get access to the App only by logging into Jira. The App uses Atlassian Connect, which relies on HTTPS and JWT authentication to secure communication between the App, the Atlassian product, and the user. Please learn more about Atlassian Connect security.

The basic HTTP authentication is used for authentication in TeamCity. The application stores the authentication data to the TeamCity servers in encrypted form. Encryption and decryption are performed using the AWS Encryption SDK engine. The encryption key is rotated yearly, and developers have no access to it.

Permissions

The maximum set of actions TeamCity Integration for Jira app may perform is expressed in the scopes in the App descriptor and is presented to the administrator during installation. This security level is enforced by Atlassian Connect and cannot be bypassed by App implementations.

Here is the list of all used scopes:

- `READ` – view, browse, and read information from Jira.
- `WRITE` – create or edit content in Jira, but not delete content.
- `DELETE` – delete content in Jira.

Learn more in the scopes documentation.

The App Interaction with Jira

The App does not store data from Jira in its tables but only updates the build and deployment data in the Development Panel in Jira. The endpoints for obtaining information about a task or project are used only for resolving a key by identifier.

The following endpoints are used:

- `POST /rest/api/3/permissions/check`
- `GET /rest/api/3/issue/{issueId}`
- `GET /rest/api/3/project/{projectId}`
- `POST /rest/builds/0.1/bulk`
- `DELETE /rest/builds/0.1/bulkByProperties`
- `POST /rest/deployments/0.1/bulk`

- `DELETE /rest/deployments/0.1/bulkByProperties`

The App Interaction with TeamCity

The App does not modify builds in TeamCity, but receive information using the following endpoints:

- `GET /app/rest/buildTypes/{btLocator}`
- `GET /app/rest/server`
- `GET /app/rest/users/{userLocator}`
- `GET /app/rest/changes`
- `GET /app/rest/builds`
- `GET /app/rest/builds/{buildLocator}`

Uptime

The App has uptime of 99.99% or higher. You can check our current and historic status at https://stats.uptimerobot.com/jqxnBSYvO3

Network and Application Security

The App hosts its infrastructure and data in Amazon Web Services (AWS) in the US East (Northern Virginia) region (us-east-1).

Failover and Disaster Recovery

Our systems were designed and built with disaster recovery in mind. Our infrastructure is spread across two AWS availability zones in one region. The live data is stored in one of these availability zones and will be recovered from the backup stored in the other zone in case of an infrastructure failure.

Backups and Monitoring

TeamCity Integration for Jira uses automation to backup all data stores that contain customer data. We back up all our critical assets and test these backups regularly to guarantee a fast recovery in case of disaster. All our backups are encrypted.

On an application level, we use logs for all activity in combination with the Datadog monitoring service. The App also uses Sentry.io, a client-side error monitoring tool that helps us discover, triage, and prioritize App errors in real-time.

Encryption

All data sent to or from TeamCity Integration for Jira systems is encrypted in transit over public networks using TLS 1.2+ with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification. We use only AWS-managed network components and policies enforcing TLS with strong ciphers and key lengths, where supported by the browser.

All data stored by the App is located in an encrypted AWS RDS instance.

Data Isolation

All customer data is stored in a secured and encrypted database. The App's compute and storage are shared among the tenants. Secure logical tenant isolation is implemented on a database level with PostgreSQL Row Level Security, which excludes the violation of isolation even in case of developer's mistake in code and ensures that no tenant can gain access to another tenant’s data.

Virtual Private Cloud

All of our servers are located within our own virtual private cloud (VPC) in a dedicated AWS account with network access controls preventing unauthorized connections to internal resources.

Data retention and removal

We retain client's data for no more than 60 days from the moment the App was deleted. If a client reinstalls the App, they have their data already pre-configured.

After 60 days since the removal of the App, all client's data is automatically deleted from the live production but remains in encrypted database backups for another 35 days.

On the expiry of 35 days, the data backups are wiped and all data will be automatically deleted forever. Every user can request the removal of usage data by contacting support or deleting his account.

You can learn more about our Data Retention Policy here.

Pentests and Vulnerability Scanning

TeamCity Integration for Jira uses third-party security tools to continuously scan for vulnerabilities and participate in the Atlassian Marketplace Bug Bounty Program for crowdsourcing vulnerability discovery.

Incident Response

TeamCity Integration for Jira implements an Incident Response Policy for handling security events which includes escalation procedures, rapid mitigation, and post mortem. All employees are informed of our policies.

Additional Security Information

Stiltsoft Europe makes an ongoing effort to reinforce good security practices and build a mature security program.

Policies

Stiltsoft Europe has developed a set of security policies covering a range of topics. These policies are updated frequently and shared with all employees.

Security awareness

All Stiltsoft Europe employees, including the TeamCity Integration for Jira team members, explore and study security aspects of web application development and exchange experience between teams on an ongoing basis.

Headquarters security

Stiltsoft Europe headquarters employs door personnel and badge access is required at all hours. Visitors are required to sign in and be escorted at all times.

Compliance

GDPR Commitment Statement

We're committed to helping TeamCity Integration for Jira users understand, and where applicable, comply with the General Data Protection Regulation (GDPR). The GDPR was designed to align and strengthen data protection laws throughout Europe to ensure that EU data subjects have greater rights regarding their personal data.

We value your trust and are dedicated to protecting your privacy.

Please see our general Privacy Policy and the App-specific Privacy Policy for more details.

Data Processing Addendum

To sign the DPA, email us at tech-support@stiltsoft.com, after which we will send you a PDF with a DPA signed by us, which you'll need to sign and send back to us.

Current TeamCity Integration for Jira Third-Party Subprocessors

For the list of the sub-possessors and the categories of data they collect please refer to our App-specific Privacy Policy.

Reporting An Issue

We appreciate your input and feedback on our security, as well as responsible disclosure.

In case you've identified a security concern, please email us at tech-support@stiltsoft.com or create a request in our support system. We'll work with you to make sure we understand the issue and address it promptly.

White hat researchers are always appreciated, and we won't take legal action against you if you act accordingly.