Vendor security-self assessment for Cloud



Alex Medved raised this on 28/Sep/22 5:09 PM

Hide details

Vendor Name

Vertuna LLC

Vendor ID

1211130

Vendor Email

sasha@vertuna.com

1a. Customer Data

We don't, except the logs. When exception occurs in rendering we store the storage format which have been used. Basically, you can connect this storage format with customer instance. Logs have a retention policy of 3 months

ConfiForms and AssetForms:

We store everything what our customer want to store in the forms they create. We ensure the data is safe and backed up (database cluster on Digital Ocean).

HTML Include - no data stored

ConfiPanel - no data stored

1b. Customer Data

NYC1 region (digital ocean) for all apps

2. Sensitive Data

3. Security Policy

4. Release Management

git with feature branches, merging to master and automatic deployment to app servers

5 Audite

6. Accreditation

7. Penetration Testing

bugcrowd initative + manual testing/code (peer) review

8. Notifying Atlassian

ConfiTemplates:

We store as little customer's data as the installing the plugin is requires us to (using spring boot Atlassian framework). Never store anything else, except the case described earlier (log files with storage format on app exceptions)

In addition to installation information we store anything what customer wants to store in the forms they create. Access to app database is restricted to app and company employees (under NDA)

10. Confidentiality

11. Managing Security Vulnerabilities

Working on bugcrowd programs and will try to formalize the process

we have a backup routine for our database, done once a day. Database backup dump is currently stored on app servers (copied from database server to app servers)

Databases run in a cluster (managed databases, with 1 stand-by mirror)

13. Data Recovery

we have only plugin installation data, a customer could reinstall the plugin in this case. All the customer's specific data is stored in their's Confluence servers (macro properties / parameters). Database cluster with 2 nodes is used for storage

For ConfiForms and AssetForms

we store the data in the database cluster, each customer has own schema (postgreSQL)

Cluster has 1 stand-by mirror

Status



Notifications on

Request type

Apply to the Security Self-Assessment program

Shared with



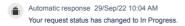
Alex Medved Creator



(Vertuna + Share

app servers are scaled horizontally, using load balancer in front. Updates are executed sequentially, removing the app server from a balancer pool to avoid downtimes

Activity







Powered by 👉 Jira Service Management