# Kintone Users & System Administration on AWS Vulnerability Assessment Results

## 1 OVERVIEW

Cybozu asked Gehirn Inc. to conduct the vulnerability assessment of Kintone Users & System Administration on AWS from November 11, 2019 to November 19. We hereby disclose the assessment results in this document.

## 2 SUMMARY OF ASSESSMENT RESULTS

No vulnerabilities were identified in this assessment.

## 3 SCOPE OF ASSESSMENT

Gehirn Inc. conducted the the assessment of Kintone Users & System Administration on AWS (released in December 2019) before its release date. Features in the scope of this assessment are as follows:

- Login function
- Customize function

## 4 ASSESSMENT CRITERIA

Gehirn Inc. assessed the product using the following criteria.

| Assessment Criteria | Details |
|---|---|
| Authentication Session Management | Assess the validity of the strength, as well as identify the problems during the authentication cycle, such as issuing authentication sessions and invalidating updates. |
| Authentication Cookie | Assess attributes attached to the Cookie, when a Cookie is used for an authentication session. |
| Assessment of Input/Output Values | Assess input/output locations that could trigger attacks, such as SQL injection, cross-site scripting, and directory traversal. |
| Verifying Validity of Requests | Assess the possibility that logged-in users or users who can execute some processes may unintentionally execute some processes by sending requests from malicious websites. |
| Logic | Assess the possibility of unauthorized use of billing, processing of loyalty points, etc. |
| Access Control | Assess the possibility that users may take some actions beyond their privileges. |

| | |
|---|---|
| Management of Important Information | Assess the validity of handling the personal information, such as passwords, credit cards, and addresses. |
| Feature to Send E-mails | As for services with a feature to send e-mails, assess the possibility that the feature may be abused to send spam e-mails by manipulating e-mail addresses and body texts, or that inconvenience may be caused by sending bulk e-mails consecutively. |