kintone mobile for Android Vulnerability Assessment Results

1 OVERVIEW

Cybozu asked Gehirn Inc. to conduct the vulnerability assessment of kintone mobile for Android from August 19, 2019 to August 22. We hereby disclose the assessment results in this document.

2 SUMMARY OF ASSESSMENT RESULTS

One vulnerability was identified in this assessment. Countermeasures against the identified vulnerability have already been provided.

3 SCOPE OF ASSESSMENT

Gehirn Inc. conducted the the assessment of kintone mobile for Android (released in August 2019). Features in the scope of this assessment are as follows:

- Login
- Logout
- Application test

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.

5 IDENTIFIED VULNERABILITIES

5.1 COUNTERMEASURES AGAINST IDENTIFIED VULNERABILITIES

We fixed the identified vulnerabilities before the release date.

5.2 IDENTIFIED VULNERABILITIES

One vulnerability was found.

Vulnerability Identification Number	CyVDB-2484
CWE	CWE-200: Information Exposure
Basic Evaluation of Vulnerability	- Attack Vector (AV): Physical - Attack Complexity (AC): Low - Privileges Required (PR): No need - User Interaction (UI): None - Scope (S): No change - Confidentiality (C): High - Integrity (I): None - Availability (A): None
CVSS v3 Base Score	4.6