Security Advisory
Database password leak

BIZERBA-SA-2023-0009

1 Summary

Authenticated users could extract the backend database password in cleartext by inspecting the webservice communication from the client to the BRAIN2 server. Attackers with a Man-In-The-Middle position could read the password only if the server was configured to use HTTP instead of HTTPS.

2 Affected Products

- BRAIN2 < 3.00

3 Mitigation

Use HTTPS connections for the communication to your BRAIN2 server.

4 Solution

Update to newest BRAIN2 version (>= 3.00)

5 Technical Details

In a specific webservice request, the server returns the database password in cleartext to the authenticated user. The issues was mitigated and the database password is never sent from the server to a client in any situation.

6 CVSS Rating

The CVSS Base Score is rated at: 6.5 (Medium)
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

7 References

8 Timeline

- 2023-09-29: New version BRAIN2 3.00 released
- 2023-09-29: Vulnerability published