Security Advisory
Three vulnerabilities in BRAIN2

BIZERBA-SA-2021-0001
March 2021

1 Overview

Three vulnerabilities have been discovered affecting the Bizerba BRAIN2 software with versions 2.36 and lower.

Bizerba rates these vulnerabilities with a CVSS v3.01 Base Score of 5.1, 6.1 and 8.8 (medium, medium and high) and strongly recommends customers to update vulnerable installations with fixed software versions.

The vulnerabilities have been discovered during internal product tests and threat analysis workshops.

2 Technical Details

2.1 Bizerba-CVE-2021-0001

- The product does not require that users must change the initial password of database within installation.
  (only relevant if SQL-Express Version is used. When specifying an own SQL database during the installation there is no default password option).

  CVSS Rating
  The CVSS v3.0 Base Score is rated at: 8.8 (high)
  CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

2.2 Bizerba-CVE-2021-0002

- For some BRAIN2 services there was no HTTPS option so the data streams within the network can be read with appropriate tools.

  CVSS Rating
  The CVSS v3.0 Base Score is rated at: 6.1 (medium)
  CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:L/I:H/A:H

2.3 Bizerba-CVE-2021-0003

- Anonymous users were allowed for BRAIN2 Touch Applications.

  CVSS Rating
  The CVSS v3.0 Base Score is rated at: 5.1 (medium)
  CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

3 Vulnerability Fix

3.1 Bizerba-CVE-2021-0001

- The MSSQL Express password of default user “sa” used during installation of BRAIN2 shall be changed.

3.2 Bizerba-CVE-2021-0002

- We recommend installing the latest BRAIN2 version 2.40.
- Change HTTP to HTTPS communication in the BRAIN2 Options.

3.3 Bizerba-CVE-2021-0003

- We recommend installing the latest BRAIN2 version 2.40.

4 Workarounds and Mitigations

4.1 Bizerba-CVE-2021-0001

- The MSSQL Express default “sa” password used during installation of BRAIN2 shall be changed. It is very important to choose a strong password for the “sa” login.

4.2 Bizerba-CVE-2021-0002

- no workaround

4.3 Bizerba-CVE-2021-0003

- no workaround

5 Affected Products

- All BRAIN2 Versions < 2.38