BIZERBA

Security Advisory
BRAIN2 version 3.04 fixes multiple vulnerabilities
BIZERBA-SA-2024-0004

1   Summary
BRAIN2 utilizes third-party software to deliver core functionality. Several npm libraries, including elliptic, ip, loader-utils, webpack, browserify-sign, css-what, glob-parent, node-forge, nth-check, semver, terser, and word-wrap, were found to have vulnerabilities. Updated versions of these libraries have been released by their providers. As a precaution and in adherence to best practices, Bizerba has decided to upgrade these components to mitigate any potential risks. BRAIN2 version 3.04 includes these updates, addressing the identified vulnerabilities.

2   Affected Products
  ▪ BRAIN2 version 3.03 and earlier

3   Mitigation
Disable the vulnerable BRAIN2 service, or implement network segmentation and firewall rules to isolate it from potential threats. Ensure unauthorized physical access to the BRAIN2 host is prevented.

4   Solution
Update BRAIN2 to the current version 3.04.

5   Technical Details
No technical details or proof-of-concept are available.

6   CVSS Rating
The CVSS Base Score is rated at: 9.8 (Critical)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

7   References

8   Timeline
  ▪ 2024-09-27: Version 3.04 released
  ▪ 2024-10-11: Vulnerability published