

Bizerba Security Advisory

Advisory Number: BIZERBA-SA-2026-0004

CVE-ID: CVE-2026-112250

Severity: Medium

CVSS v3.1 Base Score: 4.4

CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

Cleartext Storage of Windows Service Account Password in BRAIN2 Setup Log Files

1. Summary

A vulnerability has been identified in BRAIN2 versions up to and including version 3.09. Under specific installation conditions, the password of a Windows service account may be written in cleartext to a setup log file.

The issue occurs when Microsoft SQL Server access is configured using Integrated Security and the Windows account intended to run the BRAIN2 MainService is specified during execution of the BRAIN2 installation wizard.

The setup log file is stored in the temporary directory of the Windows administrator performing the installation. This directory is not accessible to standard Windows users and can generally only be accessed by users with administrative privileges.

Successful exploitation could result in the disclosure of credentials belonging to the configured BRAIN2 service account.

2. Affected Products

Product	Affected Versions	Fixed Version
BRAIN2	All versions up to and including 3.09	3.10 and later

3. Mitigation

Until an upgrade can be applied, Bizerba recommends implementing the following measures:

- Delete BRAIN2 installation log files after successful installation.

- Restrict administrative access to affected systems.
- Ensure temporary directories containing installation artifacts are adequately protected.
- Change the password of the configured service account if credential exposure is suspected.

Administrators should review and remove setup log files following the naming convention:

```
1 Bizerba
  BRAIN2_<Version>_<InstallationDate>_<InstallationTime>_setup.log
```

4. Solution

This vulnerability has been fixed in **BRAIN2 version 3.10**.

Customers are strongly advised to upgrade to **BRAIN2 version 3.10 or later**.

5. Technical Details

Vulnerability Type

CWE-532: Insertion of Sensitive Information into Log File

Description

The vulnerability is triggered when all of the following conditions are met:

1. BRAIN2 is configured to access Microsoft SQL Server using Integrated Security.
2. A Windows account is specified during execution of the BRAIN2 installation wizard.
3. The specified account is configured to run the BRAIN2 MainService Windows service.

When these conditions are met, the password of the specified Windows service account may be written in cleartext to the BRAIN2 setup log file.

The generated setup log file follows a naming convention similar to:

```
1 Bizerba
  BRAIN2_<Version>_<InstallationDate>_<InstallationTime>_setup.log
```

The file name contains the installed BRAIN2 version as well as the date and time of the installation. An example of such a file name could resemble:

```
1 Bizerba BRAIN2_3.xx.xx.x_YYYY-MM-DD_HH-MM-SS_setup.log
```

The log file is stored in the temporary directory of the Windows administrator executing the installation. Standard Windows users cannot access this directory; access is generally limited to users with administrative privileges.

Preconditions

- Local access to the affected system.
- Administrative privileges on the affected Windows system.
- Access to the temporary directory of the administrator who executed the installation.

Impact

An attacker with administrative access to the affected system may retrieve the password of the configured BRAIN2 MainService account from the installation log file.

The affected service account is required to have:

- Local Administrator privileges.
- The Windows privilege "**Log on as a service**".

Disclosure of credentials for such a privileged account can result in a significant loss of confidentiality.

6. CVSS Rating

CVSS v3.1 Base Score

4.4 (Medium)

Vector String

1 CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
--

Metric Details

Metric	Value
Attack Vector (AV)	Local (L)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	High (H)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	High (H)
Integrity (I)	None (N)
Availability (A)	None (N)

Justification

The vulnerability allows disclosure of credentials belonging to a privileged Windows service account. Exploitation requires local administrative access to the affected system and does not directly impact integrity or availability. The disclosed account possesses local administrative privileges and the Windows privilege "Log on as a service", resulting in a high confidentiality impact.

7. References

- Bizerba Security Advisory BIZERBA-SA-2026-0004
 - CVE-2026-112250
 - CWE-532: Insertion of Sensitive Information into Log File
 - Common Vulnerability Scoring System (CVSS) v3.1 Specification
-

8. Timeline

Event	Date
Vulnerability identified	2026-09-25
Fix available in BRAIN2 3.10	2026-10-02
Security Advisory published	2026-10-02

Revision History

Version	Date	Description
1.0	2026-10-21	Initial publication

Status: Ready for Information Security Office review and CVE assignment.