Security Advisory
WinCWS using static credentials

BIZERBA-SA-2024-0003

1 Summary

Credentials of local Bizerba user accounts have been compromised in recent attacks. We recommend verifying whether local Bizerba accounts are present on all systems running WinCWS and, if applicable, immediately changing the associated passwords to mitigate the risk of unauthorized access and ensure the integrity and security of your systems.

2 Affected Products

- WinCWS installations before October 2024

3 Mitigation

Disable remote access services, or implement network segmentation and strict firewall rules to isolate the device from potential threats and unauthorized access.

4 Solution

Update the passwords for all user accounts associated with Bizerba software and technicians. It is recommended to assign unique credentials to each account. Ensure that the accounts are configured as local user accounts only, and that remote services are not accessible via the internet for enhanced security.

5 Technical Details

During the installation process for the software WinCWS often static credentials were used to create local user accounts on the Windows host computer. This is not an issue of the software itself, but of the manual installation process performed by service technicans. The credentials of the user are used to set up a scheduled task and were potentially extracted by an attacker using mimikatz.

6 CVSS Rating

The CVSS Base Score is rated at: 7.8 (High)
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

7 References

8 Timeline

- 2024-09-19 Vulnerability reported
- 2024-09-19 Manual changed and service technicans instructed to inform costumers
- 2024-10-11: Vulnerability published