Security Advisory
Secure Update Process Enhancement for Labeler and Checkweigher

BIZERBA-SA-2023-0002

1 Summary

The secure update process employed by our software has been strengthened with enhanced asymmetric cryptography methods. While there is no evidence to suggest that the former key was compromised, we have taken proactive measures to maintain the confidentiality of the private key. In the latest software version, we have introduced a new public/private key pair, effectively replacing the previous keys. This update mitigates the potential risk of attackers utilizing the private key to sign and distribute malicious updates, thereby preserving the integrity and confidentiality of the devices. Our investigation into the attack on the Bizerba.com domain has not revealed any evidence or indications of private key compromise.

2 Affected Products

- Software GT-SoftControl < 6.0
- Lingx < 13
- Device firmware for product families CWx and GLx < 16.0

3 Mitigation

- Disable the FTP and SFTP services.
- Prevent unauthorized physical access to the devices.

4 Solution

Update software to the current version of the corresponding software.

5 Technical Details

If exploited, this vulnerability poses a significant security risk to the affected devices. By utilizing a compromised private key, an attacker could maliciously sign software updates, leading to the installation of unauthorized and potentially harmful software. As a result, the confidentiality and integrity of the affected devices may be compromised, potentially exposing sensitive data and allowing unauthorized access to the compromised systems.

6 CVSS Rating

The CVSS v3.1 Base Score is rated at: 8.1 (High)
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

7 References

8 Timeline

- 2023-07-12: Vulnerability published