Security Advisory
Vulnerability in third-party component of iS30/iS50 weighing terminals

BIZERBA-SA-2022-0001
January 2022

1 Summary

A vulnerability has been discovered affecting the third-party software component CODESYS V3 web server. If this optional component is used specific crafted requests may cause a heap-based buffer overflow. Further on this could crash the web server, lead to a denial-of-service condition or may be utilized for remote code execution.

Bizerba rates these vulnerabilities with CVSS v3.0 Base Score at: 10.0 (Critical)
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

2 Affected Products

- iS30 before version 1.22.1, with WebVisu license
- iS50 before version 2.28.1, with WebVisu license

3 Solution and Mitigations

If the optional license for the WebVisu module was not purchased, no measures need to be taken, because the vulnerable component is not installed by default.

Mitigation

To mitigate the risk, isolate the affected devices or block connections to port TCP/8080 with additional firewall.

Solution

Please update your device to the latest version (1.22.1 for iS30 and 2.28.1 for iS50). Since version CODESYS V3.5 SP11 was updated to version V3.5 SP17 which not vulnerable anymore.

4 Technical Details

The third-party component CODESYS web server (WebVisu) is affected by the vulnerability CVE-2020-10245 in all versions prior V3.5.15.40. More technical details are published by the advisory[1] of the manufacturer.

5 References

[1] “Advisory2020-03_CDS-69655_01.pdf” from 3S-Smart Software Solutions GmbH
https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13078&token=de344ca65252463cc581ef144e0c53bd97b8f211&download=

6 History

- 23 Sep 2021: Vulnerability reported
- 17 Jan 2022: Provide solution as update package (1.22.1 for iS30 and 2.28.1 for iS 50)
- 17 Jan 2022: Security Advisory published