Security Advisory
Hardening of remote access services for retail scales

BIZERBA-SA-2023-0006

1 Summary

The SSH, SFTP, FTPS and XRDP services have been hardened by changing the default configuration.

2 Affected Products

- Q1 scales with Linux OS image bizDebOS_v13.04_b0004 and previous
- K3 scales with Linux OS image bizRLPOS_v11.04_b0001 and previous
- XC scales with Linux OS image bizLPOS_v9.14_b0001 and previous
- KH2 scales with Linux OS image bizLPOS_v8.17_b0001 and previous

3 Mitigation

- Disable the XRDP service
- Prevent access to port 3389/tcp by external firewall
- Separate device to isolated VLAN

4 Solution

Update OS to the current version or install vulnerability patch bizvulnerabilitypatch_1.20.0002.

5 Technical Details

Due to a misconfiguration of the SSH/SFTP service, the front-end user could perform remote logins to the scales. Even if this user is password protected, remote login is not required and has been disabled by default in the latest patch. The configuration of the XRDP and SFTP services on retail scales (K3, Q1) was not hardened and offered legacy encryption ciphers [1,2]. More information is available in the software change document [3].

6 CVSS Rating

The CVSS Base Score is rated at: 7.5 (High)
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

7 References

[1] https://www.openssl.org/blog/blog/2016/08/24/sweet32/
[2] https://www.tenable.com/plugins/nessus/65821
[3] more information see the software change document bizretail_security_release_v107_b0002_lin_38120592007

8 Timeline

- 2023-05-02: Vulnerability reported
- 2023-06-15: Patch developed
- 2023-08-01: Patch released
- 2023-10-10: Vulnerability published