Security Advisory
Remote Code Execution without authentication

BIZERBA-SA-2024-0001

1 Summary

Attackers have the potential to execute commands at scale without authentication. The RetailDeviceServer as vulnerable component is specifically designed for the remote control of devices, making remote code execution an inherent feature. However, earlier versions of PowerScale (versions prior to 3.54) are using a RetailDeviceServer (version < 2.53) whichs lacks authentication. Additionally, due to a configuration error, version 2.81 of RetailDeviceServer on the RetailStore device is missing authentication. RDS versions preceding 2.81 or succeeding 2.81 are not affected. Furthermore, RetailDeviceServer version 2.81.10 on PowerScale devices is not impacted.

2 Affected Products

- Retail scales with PowerScale <= 3.53 which are using RetailDeviceServer < 2.53
- Retail scales with RetailStore (K3, KH class) which are using RetailDeviceServer in version 2.81

Vulnerable RetailDeviceServer versions

RetailStore [Version]	Q1 [RDS Version]	K3 Linux [RDS Version]	K3 Windows [RDS Version]
1.6.0	2.80.3	2.81.0004	2.81.0004
1.6.1	2.80.3	2.81.0004	2.81.0004
1.7.0	2.80.3	2.81.12	2.81.12
1.7.1	2.80.3	2.82.2	2.81.12
1.7.2	2.80.3	2.82.2	2.81.12
1.8.0	2.80.3	2.83.2	2.81.12

Vulnerable
NOT vulnerable

3 Mitigation

Block network port 7080 for all devices by external firewall.

4 Solution

Update retail scales with PowerScale to the current version 3.54 or use a version of RetailDeviceServer >= 2.53. For retail scales with RetailStore version <= 1.8.0 update the RetailDeviceServer to the current version >= 2.83 or the RetailStore version to the current version 1.8.1.

5 Technical Details

No technical details or proof-of-concept are available.

6 CVSS Rating

The CVSS Base Score is rated at: 10.0 (Critical)
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

7 References

8 Timeline

- 2024-06-14: Vulnerability reported
- 2024-06-19: Patch RetailDeviceServer 2.8.3 released
- 2024-06-24: Patch RetailStore 1.8.1 released
- 2024-06-28: Advisory released