December 1, 2023

Overall rating: Medium

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of BD FACSChorus vulnerabilities impacting Healthcare and Public Health sectors. The vulnerability affects BD FACSChorus - HP Z2 G9 workstation, shipped with FACSDiscover S8 Cell Sorter: v5.0 and v5.1 and BD FACSChorus - HP Z2 G5 workstation, shipped with FACSMelody Cell Sorter: v3.0 and v3.1.

Technical Details

In BD FACSChorus v5.0, v5.1, v3.0, and v3.1, the respective workstation operating system does not restrict what devices can interact with its USB ports. If exploited, a threat actor with physical access to the workstation could gain access to system information and potentially exfiltrate data. Additionally, the operating system hosting the FACSChorus application is configured to allow transmission of hashed user credentials upon user action without adequately validating the identity of the requested resource. This is possible using LLMNR, MBT-NS, or MDNS and will result in NTLMv2 hashes being sent to a malicious entity position on the local network. These hashes can subsequently be attacked through brute force and cracked if a weak password is used. This attack would only apply to domain joined systems.

In BD FACSChorus v5.0 and v5.1, the software contains sensitive information stored in plaintext. A threat actor could gain hardcoded secrets used by the application, which include tokens and passwords for administrative accounts.

In BD FACSChorus v5.0 and v5.1, the software database can be accessed directly with the privileges of the currently logged-in user. A threat actor with physical access could potentially gain credentials, which could be used to alter or destroy data stored in the database. Additional privilege issues in BD FACSChorus v5.0 and v5.1 and the respective workstations, the software does not properly assign data access privileges for operating system user accounts. A non-administrative OS account can modify information stored in the local application data folders.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **MEDIUM** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-29060, CVE-2023-29061, CVE-2023-29062, CVE-2023-29063, CVE-2023-29064, CVE-2023-29065, CVE-2023-29066
- ICSMA-23-331-01 BD FACSChorus
- VRM Vulnerability Reports