Title:

Insecure storage of login data for database connections in FlexPro: Security risk assessment

Description:

A connection to an SQL server is established via a connection string, which contains the user name and password in the event that the SQL server itself authorizes the connection. These connection strings were stored unencrypted in FlexPro.

If the connection to the SQL Server is authorized via a Windows account, the connection string does not contain a password. Such connections are therefore not affected by this security problem.

In detail, the following types of server connections are affected:

a) Data import from SQL databases via ODBC
b) Server-based indexing of measurement data for the FlexPro Data Explorer
c) Connection to the ASAM ODS server via the CORBA interface

Affected Versions:

Software Name:

a) FlexPro (all versions up to and including 14.0.7 and 13.0.24)
b) FlexPro Professional with Data Explorer option and FlexPro Developer Suite (all versions up to and including 14.0.7 and 13.0.24)
c) FlexPro Professional with ASAM ODS option and FlexPro Developer Suite (versions from 8.0.1 up to and including 14.0.7 and 13.0.24)

Environment:

- Windows 32-bit and 64-bit

Impact:

If compromised, an attacker would gain access to the SQL databases that are configured for authorization using SQL Server authentication. . Depending on the permissions granted to this login, the attacker may have the ability to read, modify, or delete data, execute arbitrary queries, and potentially escalate privileges within the database environment.

Identification:

The versions of FlexPro 2025 from version 14.0.8 and FlexPro 2021 from version 13.0.25 check all existing connection strings when starting FlexPro and when opening a project database and, if a password is included, isolate and store it encrypted with the user's Windows account. If a password is found, FlexPro displays a message.

Severity:

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Score:

6.5 (medium) if the SQL Server authentication login has read-only access.
7.5 (high) if the SQL Server authentication login has read/write access.

Remediation Recommendation:

1. Update to FlexPro 14.0.8 or 13.0.25.
2. If possible, switch all database connections used by FlexPro from SQL Server authentication to Windows authentication.
3. Change the passwords of server connections with SQL Server authentication that are used by FlexPro.

References:

- OWASP Top 10 A02:2021 (Cryptographic Failures)
- NIST SP 800-63B Digital Identity Guidelines