Security Advisory: Two vulnerabilities in Bosch Fire Monitoring System (FSM) – January 2021

BOSCH-SA-332072-BT

1 Overview and Management Summary

Two vulnerabilties have been discovered affecting the Bosch Fire Monitoring System (FSM-2500 and FSM-5000). The critical issue applies to FSM systems with versions 5.2 and lower.
Bosch rates these vulnerabilities with a CVSS v3.1 Base Score of 4.4 and 10.0 (medium and critical) and strongly recommends customers to update vulnerable components with fixed software versions.
The vulnerabilities have been discovered during internal product tests.

2 Technical Details

2.1 CVE-2020-6779

Use of Hard-coded Credentials in the database of Bosch FSM-2500 server and Bosch FSM-5000 server up to and including version 5.2 allows an unauthenticated remote attacker to log into the database with admin-privileges. This may result in complete compromise of the confidentiality and integrity of the stored data as well as a high availability impact on the database itself. In addition, an attacker may execute arbitrary commands on the underlying operating system.

2.1.1 Vulnerability Classification and Solution Approach

This vulnerability is classified as “CWE-798: Use of Hard-coded Credentials".

2.1.2 CVSS Rating

The CVSS v3.1 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

2.2 CVE-2020-6780

Use of Password Hash With Insufficient Computational Effort in the database of Bosch FSM-2500 server and Bosch FSM-5000 server up to and including version 5.2 allows a remote attacker with admin privileges to dump the credentials of other users and possibly recover their plain-text passwords by brute-forcing the MD5 hash.

2.2.1 Vulnerability Classification and Solution Approach

This vulnerability is classified as “CWE-916: Use of Password Hash With Insufficient Computational Effort”.

2.2.2 CVSS Rating

The CVSS v3.1 Base Score is rated at: **4.4 (medium)**
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N

3 Vulnerability Fix

The recommended approach is to update the software of affected Bosch products (see chapter 5).

If an update is not possible in a timely manner, the temporary workaround can be utilized (see chapter 4).

4 Mitigations and Workarounds

4.1 Company network

It is recommended that the workstation used to install FSM server shall not be logged onto a company network – neither before nor during or after installation.
It is recommended to disable the ability of the Windows operating system to cache credentials on any device, where credentials are not needed. Evaluate your servers and workstations to determine the requirements.

4.2 MSSQL Express

Reset the SQL system administrator password and change the SQL Connection password accordingly in the FSM System configuration (see TI 2265/2019 from BT-FIR distributed in December 2019).

The default “sa” password used during installation of the SQL express database shall be changed.
It is very important to choose a strong password for the “sa” login.

Suggested procedure for changing the SQL System Administrator password:

A. Reset the SQL system administrator password
   a) Download and install Microsoft SQL Server Management Studio Express;
   Make sure to choose the suitable Windows platform (x86 or x64);
   b) Open the application, and choose the authentication mode: “Windows Authentication”;
   c) Press “Connect” button and navigate to the Security -> Logins folder in the left side of your window; Right-click on “sa” and choose properties;
   d) Change the password with a complex one.
   e) Make sure that SQL Server allows the “sa” account to connect and has enough permissions;
   Navigate to Status -> and choose “Grant” and “Enabled” in the right side of the window.
   f) Press OK and exit Microsoft SQL Server Management Studio Express
B. Change SQL System Administrator password in the FSM System configuration;
   a) Stop the service FSM Server in Windows Task Manager.
   b) Run the FSM System Configuration program (from Start Menu).
   c) Open the “Database” tab, put the new password in the field and try “test connection” to check that everything is ok.
   d) If the connection is online, press OK button.
   e) Run the service FSM Server in Windows Task Manager.

5 Affected Software

5.1 Bosch Fire Monitoring System (FSM)

For Bosch Fire Monitoring System (FSM) the following patches are strongly recommended:

FSM versions	Affected versions	Fixed versions
FSM-2500	5.2 and lower	5.6 and higher
FSM-5000	5.2 and lower	5.6 and higher

Download area – Server installation file
Download area – Client installation file

6 Direct Links

Bosch Building Technologies Security Advisory page
Bosch PSIRT

7 Document Change Log

2021-Jan-20 – Revision 1.00: Initial Release