Bosch Fire Monitoring System (FSM) affected by log4net Vulnerability
BOSCH-SA-479793-BT

1 Advisory Information

- **Advisory ID:** BOSCH-SA-479793-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2018-1285
    - Base Score: 9.8 (Critical)
    - Environmental Score: 6.7 (Medium)
- **Published:** 23 Mar 2022
- **Last Updated:** 23 Mar 2022

2 Summary

A vulnerability has been discovered affecting the Bosch Fire Monitoring System (FSM-2500, FSM-5000, FSM-10k and obsolete FSM-10000). The issue applies to FSM server with version 5.6.630 and lower, and FSM client with version 5.6.2131 and lower. Bosch recommends customers to update vulnerable components with the provided patch. The vulnerability has been discovered in field.

The vulnerability CVE-2018-1285 in the affected component Apache log4net is rated with a CVSS v3.1 Base Score of 9.8 (critical), but the exploitability is reduced in a proper installation of Fire Monitoring System (FSM): local system access with administrative access rights is required to exploit the vulnerability. This leads to a lower Environmental/Overall CVSS v3.1 Score of 6.7 (medium).

3 Affected Products

- Bosch FSM-10000 Client <= 5.6.2131
- Bosch FSM-10000 Server <= 5.6.630
- Bosch FSM-10k Client <= 5.6.2131
- Bosch FSM-10k Server <= 5.6.630
- Bosch FSM-2500 Client <= 5.6.2131
- Bosch FSM-2500 Server <= 5.6.630
- Bosch FSM-5000 Client <= 5.6.2131
- Bosch FSM-5000 Server <= 5.6.630

4 Solution and Mitigations

4.1 Software Patch for FSM 5.6

A software patch is available to fix FSM server 5.6.630 and FSM client 5.6.2131. Upon execution it will temporarily stop the FSM server and replace the affected Apache log4net component.

A successful update can be verified by checking the log4net version information in the About-menu or via file properties of log4net.dll in installation folders.

© Robert Bosch GmbH 2022. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

4.2 Software Update

Update to a version of FSM server higher than 5.6.630 and FSM client higher than 5.6.2131.

5 Vulnerability Details

5.1 CVE-2018-1285

CVE description: Apache log4net versions before 2.0.10 do not disable XML external entities when parsing log4net configuration files. This allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.

- Problem Type:
  - CWE-611
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:X/IR:X/AR:X/MAV:L/MAC:X/MPR:H/MUI:X/M
  - Base Score: 9.8 (Critical)
  - Environmental Score: 6.7 (Medium)

6 Remarks

6.1 Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g. in this security advisory.

6.2 CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

7 Additional Resources

- [1] FSM 5.6 Server Patch: `https://downloadstore.boschsecurity.com/FILES/Patch_FSM_5_6_Server.zip`
- [2] FSM 5.6 Client Patch: `https://downloadstore.boschsecurity.com/FILES/Patch_FSM_5_6_Client.zip`

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: `psirt@bosch.com`.

© Robert Bosch GmbH 2022. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

8 Revision History

- 23 Mar 2022: Initial Publication

© Robert Bosch GmbH 2022. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.