1 Advisory Information

- **Advisory ID:** BOSCH-SA-013924-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2022-36301
    - Base Score: 9.8 (Critical)
  - CVE-2022-36302
    - Base Score: 8.8 (High)
- **Published:** 01 Aug 2022
- **Last Updated:** 01 Aug 2022

2 Summary

Multiple vulnerabilities were identified in BF-OS version 3.x up to and including 3.83 used by Bigfish V3 and PR21 (Energy Platform) devices and Bigfish VM image, which are part of the data collection infrastructure of the Energy Platform solution.

The most critical vulnerability may allow an unauthenticated remote attacker to gain administrative privileges to the device by brute-forcing a weak password. The second vulnerability may allow a remote authenticated attacker to gain unauthorized read access to local operating system files outside the web server root.

Both vulnerabilities are closed with BF-OS version 3.84, which Bosch will install remotely to affected customers after agreeing on a suitable maintenance window. Affected customers do not have to take further action.

The vulnerabilities were identified in an internal penetration test. Bosch is currently not aware of exploitation of these vulnerabilities in the wild.

3 Affected Products

- Bosch BF-OS 3.0 <= 3.83 on: Bigfish V3 (Linux)
- Bosch BF-OS 3.0 <= 3.83 on: PR21 (Linux)
- Bosch BF-OS 3.0 <= 3.83 on: VM (Windows)

4 Solution and Mitigations

4.1 Software Update

Update to BF-OS version 3.84 or greater to close these vulnerabilities.

Bosch will contact all affected customers individually and push this new version to affected devices after having agreed on a customer-specific maintenance window. The installation takes approximately half an hour and during this time measurement data cannot be captured.

The update results in the following changes to the affected devices:

- The devices will enforce a sufficiently long and complex password to protect against unauthorized access.

- Each customer will receive a list of new initial passwords for his devices.
- Connecting to a device from the Energy Platform software requires entering the device password.

Customers can verify that the update has been installed successfully by verifying the version in the device overview of the Energy Platform software.

5 Vulnerability Details

5.1 CVE-2022-36301

CVE description: BF-OS version 3.x up to and including 3.83 do not enforce strong passwords which may allow a remote attacker to brute-force the device password.

- Problem Type:
  - CWE-521 Weak Password Requirements
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.2 CVE-2022-36302

CVE description: File path manipulation vulnerability in BF-OS version 3.00 up to and including 3.83 allows an attacker to modify the file path to access different resources, which may contain sensitive information.

- Problem Type:
  - CWE-641 Improper Restriction of Names for Files and Other Resources
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

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

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

8 Revision History

- 01 Aug 2022: Initial Publication