Several Vulnerabilities in Bosch B426, B426-CN/B429-CN, and B426-M

BOSCH-SA-196933-BT

1 Advisory Information

- **Advisory ID:** BOSCH-SA-196933-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-23845
    - Base Score: 8.0 (High)
  - CVE-2021-23846
    - Base Score: 8.8 (High)
- **Published:** 28 May 2021
- **Last Updated:** 28 May 2021

2 Summary

A security vulnerability affects the Bosch B426, B426-CN/B429-CN, and B426-M. The vulnerability is exploitable via the network interface. Bosch rates this vulnerability at 8.0 (High) and recommends customers to update vulnerable components with fixed software versions.

A second vulnerable condition was found when using http protocol, in which the user password is transmitted as a clear text parameter. Latest firmware versions allow only https.

If a software update is not possible in a timely manner, a reduction in the systems network exposure is advised. Internet-accessible systems should be firewalled. Additional protective steps like network isolation by VLAN.

These vulnerabilities were reported by Chizuru Toyama of TXOne IoT/ICS Security Research Labs.

2.1 Impact

Under certain circumstances, a malicious or unintended user could gain access to the B426 web server and access the configuration pages without needing to enter login credentials.

3 Affected Products

- Bosch B426 Firmware < 03.08
  - CVE-2021-23845
- Bosch B426-CN/B429- CN Firmware < 03.08
  - CVE-2021-23845
- Bosch B426-M Firmware < 03.10
  - CVE-2021-23845
- Bosch B426 Firmware 03.01.0004
  - CVE-2021-23846
- Bosch B426 Firmware 03.02.002

- CVE-2021-23846
- Bosch B426 Firmware 03.03.0009
  - CVE-2021-23846
- Bosch B426 Firmware 03.05.0003
  - CVE-2021-23846

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the software of affected Bosch products to a fixed version. If an update is not possible in a timely manner, the mitigation approaches Firewalling and IP Filtering can be utilized. A list of affected and fixed firmware versions is available in the “Affected Products” section of this document. A fixed B426, B426-CN/B429-CN and B426-M versions are available on the Bosch Product Catalog

4.2 Firewalling (Network)

It is advised that the devices should not be exposed directly to the internet or other insecure networks. This includes port-forwarding, which would not protect devices adequately. Firewalling a device significantly reduces its attack surface.

4.3 Other

Ensure that the “Web and Automation Security” setting for the B426 is enabled.

5 Vulnerability Details

5.1 CVE-2021-23845

CVE description: This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019.

- Problem Type:
  - CWE-284 Improper Access Control
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.0 (High)

5.2 CVE-2021-23846

CVE description: When using http protocol, the user password is transmitted as a clear text parameter for which it is possible to be obtained by an attacker through a MITM attack.

This will be fixed starting from Firmware version 3.11.5, which will be released on the 30th of June, 2021.

- Problem Type:
  - CWE-319 Cleartext Transmission of Sensitive Information
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

5.3 Remark

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.

6 Additional Resources

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

7 Revision History

- 28 May 2021: Initial Publication