Multiple vulnerabilities in Bosch AMC2 (Access Modular Controller)
BOSCH-SA-940448-BT

BOSCH
Invented for life

1 Advisory Information

- **Advisory ID:** BOSCH-SA-940448-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-23842
    - Base Score: 5.7 (Medium)
  - CVE-2021-23843
    - Base Score: 8.8 (High)
- **Published:** 19 Jan 2022
- **Last Updated:** 28 Jan 2022

2 Summary

The Bosch AMC2 (Access Modular Controller) is an door access controller. It takes access control decisions for a group of up to eight access points. These access points may consist of doors, gates, barriers, turn stiles, revolving doors, man-traps, ID card readers, door opening elements and sensors. The device is designed for fully process the access logic at the assigned entrances.

Two discovered security vulnerabilities allow an unauthenticated attacker to decrypt network traffic and change device configuration. This affects Bosch products Building Integration System (BIS), Access Management System (AMS), Access Professional Edition (APE), and Access Modular Controller (AMC2).

For more details please see the description of the vulnerabilities in this advisory.

Bosch rates the vulnerabilities CVE-2021-23842 and CVE-2021-23843 with a CVSS v3.1 Base Score of 5.7 (Medium) and 8.8 (High) respectively. The actual rating depends on the individual vulnerability and the final rating on the customer's environment.

Customers are strongly advised to update to the fixed versions or consider listed mitigation.

Both vulnerabilities were discovered by external security researcher Alexander Nochvay of Kaspersky.

3 Affected Products

- Bosch AMC2
- Bosch AMS < 4.0
- Bosch APE <= 3.8.x
- Bosch BIS < 4.9.1

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the affected Bosch software to an improved version. The latest versions BIS 4.9.1 and AMS 4.0 are immune against the discovered vulnerabilities CVE-2021-23842 and CVE-2021-23843.

© 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.

This update will change the communication between controllers and backend and will introduce DTLS communication for AMS and BIS.

Please note that AMS and BIS will update AMC2 controllers with a strengthened firmware automatically. Please refer to technical documentation in the software release for more details.

There is a patch for APE addressing CVE-2021-23843. If you want to address also CVE-2021-23842 then we recommend to migrate the APE installation to AMS 4.0 or BIS 4.9.1.

4.2 Mitigations

We recommend to update AMS and BIS to version 4.0 resp. 4.9.1 immediately as described in section Software Updates. This will address both vulnerabilities CVE-2021-23842 and CVE-2021-23843.

For AMS and BIS installations which cannot be updated to version 4.0 resp. 4.9.1 immediately, Bosch has prepared patches which will distribute a hardened firmware to the AMC2 door controllers. This patch addresses CVE-2021-23843.

For APE 3.8.x installations there is a patch addressing CVE-2021-23843.

Please notice that the patch will reduce convenience of the AMC2 configuration. Please refer to the patches' technical documentation for details.

If you want to reduce the security risk further, we recommend to follow general IT hardening guidelines and especially operate access control in a secured local area network.

5 Vulnerability Details

5.1 CVE-2021-23842

CVE description: Communication to the AMC2 uses a state-of-the-art cryptographic algorithm for symmetric encryption called Blowfish. An attacker could retrieve the key from the firmware to decrypt network traffic between the AMC2 and the host system.

Thus, an attacker can exploit this vulnerability to decrypt and modify network traffic, decrypt and further investigate the device's firmware file, and change the device configuration.

The attacker needs to have access to the local network, typically even the same subnet.

- Problem Type:
  - CWE-321 Use of Hard-coded Cryptographic Key
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
  - Base Score: 5.7 (Medium)

5.2 CVE-2021-23843

CVE description: The Bosch software tools AccessIPConfig.exe and AmcIpConfig.exe are used to configure certains settings in AMC2 devices. The tool allows putting a password protection on configured devices to restrict access to the configuration of an AMC2. An attacker can circumvent this protection and make unauthorized changes to configuration data on the device.

© 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.

An attacker can exploit this vulnerability to manipulate the device's configuration or make it unresponsive in the local network.

The attacker needs to have access to the local network, typically even the same subnet.

- Problem Type:
  - CWE-306 Missing Authentication for Critical Function
- CVSS Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/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

- [1] Software Updates: https://downloadstore.boschsecurity.com
- [2] BIS Download Area: https://downloadstore.boschsecurity.com/index.php?type=BIS
- [3] AMS Download Area: https://downloadstore.boschsecurity.com/index.php?type=AMS
- [4] APE Download Area: https://downloadstore.boschsecurity.com/index.php?type=APE

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

7 Revision History

- 28 Jan 2022: Updated affected hardware list
- 19 Jan 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.

8 Appendix

8.1 Affected Software

8.1.1 Bosch Building Integration System (BIS)

Family Name	CTN	SAP#	Material description
Building Integration System 4.6	BIS-FACE-BPA46	F.01U.351.041	BIS Access Engine 4.6 Basic license
Building Integration System 4.7	BIS-FACE-BPA47	F.01U.363.020	BIS Access Engine 4.7 Basic license
Building Integration System 4.8	BIS-FACE-BPA48	F.01U.386.762	BIS Access Engine 4.8 Basic license
Building Integration System 4.9	BIS-FACE-BPA49	F.01U.395.613	BIS Access Engine 4.9 Basic license

8.1.2 Bosch Access Management System (AMS)

Family Name	CTN	SAP#	Material description
Access Management System 2.0	AMS-BASE-LITE20	F.01U.363.047	AMS 2.0 Lite license
Access Management System 2.0	AMS-BASE-PLUS20	F.01U.363.048	AMS 2.0 Plus license
Access Management System 2.0	AMS-BASE-PRO20	F.01U.363.049	AMS 2.0 Pro license
Access Management System 3.0	AMS-BASE-LITE30	F.01U.386.724	AMS 3.0 Lite license
Access Management System 3.0	AMS-BASE-PLUS30	F.01U.386.725	AMS 3.0 Plus license
Access Management System 3.0	AMS-BASE-PRO30	F.01U.386.726	AMS 3.0 Pro license

8.1.3 Bosch Access Professional Edition (APE)

Family Name	CTN	SAP#	Material description
Access PE	ASL-APE3P-BASE	F.01U.298.461	Access PE - Basic License
Access PE	ASL-APE3P-BEXT	F.01U.298.462	Access PE - Extended License

8.2 Affected Hardware

8.2.1 Bosch AMC2 Controllers

Family Name	CTN	SAP#	Material description
AMC2 Doorcontroller	APC-AMC2-2WCF	F.01U.371.285	AMC2 Doorcontroller WI, 2 readers
AMC2 Doorcontroller	APC-AMC2-4R4CF	F.01U.027.206	AMC2 Doorcontroller RS485 with CF Card
AMC2 Doorcontroller	APC-AMC2-4WCF	F.01U.027.201	AMC2 Doorcontroller 4 Wiegand with CF Card
AMC 2 Doorcontroller	API-AMC2-16ION	F.01U.013.384	Standalone controller for BIS with OPC

© 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.