

Sensitive information disclosure in Bosch Configuration Manager

BOSCH-SA-981803-BT

Advisory Information

Advisory ID: BOSCH-SA-981803-BT

CVE Numbers and CVSS v3.1 Scores:

[CVE-2024-98763](#)

Base Score: [8.4 \(High\)](#)

Published: 01 Oct 2024

Last Updated: 01 Oct 2024

Summary

A vulnerability was discovered during internal testing of the Bosch Configuration Manager, which may temporarily store sensitive information of the configured system.

Affected Products

Bosch Configuration Manager

CVE-2024-98763

Version(s): 7.72.0106

Solution and Mitigations

Software Update

The recommended approach is to update the affected Bosch Configuration Manager to the fixed version 7.72.0128.

The version of the Configuration Manager should be checked after the update to confirm successful installation, e.g. on the splash screen on startup or in the Help -> About menu.

Vulnerability Details

CVE-2024-98763

CVE description: Information disclosure in Bosch Configuration Manager in Version 7.72.0106 allows an attacker to access sensitive information.

Problem Type:

[CWE-312 Cleartext Storage of Sensitive Information](#)

CVSS Vector String: [CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N](#)

Base Score: 8.4 (High)

Remarks

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.

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.

Additional Resources

[1] Bosch Download Area: <https://downloadstore.boschsecurity.com/?type=CM>

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

Revision History

01 Oct 2024: Initial Publication

Appendix

Material Lists

Bosch Configuration Manager

Family Name	CTN	SAP#	Material Description
Configuration Tools	MFT-CM	F.01U.360.102	Free of charge configuration tool