1 Advisory Information

- **Advisory ID:** BOSCH-SA-446276-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-23850
    - Base Score: 6.8 (Medium)
  - CVE-2021-23851
    - Base Score: 6.8 (Medium)
- **Published:** 30 Mar 2022
- **Last Updated:** 08 Apr 2022

2 Summary

A recently discovered security vulnerability allows an attacker to cause an buffer overflow in the recovery image, crashing the application and open the possibility for code execution.

The recovery image can only be booted using a command requiring administrative access or requiring physical access to the device.

Bosch rates this vulnerability with CVSSv3.1 base scores of 6.8 (Medium).

The actual rating depends on the final rating specific to each customer's environment.

Customers are advised to upgrade to the fixed version.

The vulnerability was discovered by Andrey Muravitsky from Kaspersky ICS CERT.

3 Affected Products

- Bosch CPP Firmware on: CPP4, CPP6, CPP7, CPP7.3

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the affected Bosch software to a fixed version.

The update of the recovery image does not impact the operation of the normal firmware image, but a reboot of the camera is required after upload.

It is recommended to check the success of the update by calling `https://device-name-or-ip/version` after the update.

The app0 version after the update must list:

version_major: 7

version_minor: 81

build: 60

More information about the update process and version checking can be retrieved from the Bosch Community at:

https://community.boschsecurity.com/t5/Security-Video/Update-the-recovery-image-based-on-Security-Advisory-BOSCH-SA/ta-p/54705

5 Vulnerability Details

5.1 CVE-2021-23850

CVE description: A specially crafted TCP/IP packet may cause a camera recovery image telnet interface to crash. It may also cause a buffer overflow which could enable remote code execution.

The recovery image can only be booted with administrative rights or with physical access to the camera and allows the upload of a new firmware in case of a damaged firmware.

- Problem Type:
  - CWE-121 Stack-based Buffer Overflow
- CVSS Vector String: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 6.8 (Medium)

5.2 CVE-2021-23851

CVE description: A specially crafted TCP/IP packet may cause the camera recovery image web interface to crash. It may also cause a buffer overflow which could enable remote code execution.

The recovery image can only be booted with administrative rights or with physical access to the camera and allows the upload of a new firmware in case of a damaged firmware.

- Problem Type:
  - CWE-121 Stack-based Buffer Overflow
- CVSS Vector String: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 6.8 (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] Firmware Download Area: https://downloadstore.boschsecurity.com/index.php?type=FW

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

8 Revision History

- 08 Apr 2022: Added description to check if update was successful
- 30 Mar 2022: Initial Publication

9 Appendix

9.1 Affected Plattforms and Cameras

CPP7.3

- AUTODOME IP 4000i
- AUTODOME IP 5000i
- AUTODOME IP starlight 5000i (IR)
- AUTODOME IP starlight 7000i
- DINION IP 3000i
- DINION IP bullet 4000i
- DINION IP bullet 5000
- DINION IP bullet 5000i
- DINION IP bullet 6000i
- FLEXIDOME IP 3000i
- FLEXIDOME IP 4000i
- FLEXIDOME IP 5000i
- FLEXIDOME IP starlight 5000i (IR)
- FLEXIDOME IP starlight 8000i
- MIC IP starlight 7000i
- MIC IP starlight 7100i
- MIC IP ultra 7100i
- MIC IP fusion 9000i

CPP7

- DINION IP starlight 6000
- DINION IP starlight 7000
- DINION IP thermal 8000
- FLEXIDOME IP starlight 6000
- FLEXIDOME IP starlight 7000
- DINION IP thermal 9000 RM

CPP6

- AVIOTEC IP starlight 8000
- DINION IP starlight 8000 12MP
- DINION IP ultra 8000 12MP
- DINION IP ultra 8000 12MP with C/CS mount telephoto lens
- FLEXIDOME IP panoramic 6000 12MP 180
- FLEXIDOME IP panoramic 6000 12MP 360
- FLEXIDOME IP panoramic 6000 12MP 180 IVA
- FLEXIDOME IP panoramic 6000 12MP 360 IVA
- FLEXIDOME IP panoramic 7000 12MP 180

- FLEXIDOME IP panoramic 7000 12MP 360
- FLEXIDOME IP panoramic 7000 12MP 180 IVA
- FLEXIDOME IP panoramic 7000 12MP 360 IVA

CPP4

- AUTODOME IP 4000 HD
- AUTODOME IP 5000 HD
- AUTODOME IP 5000 IR
- AUTODOME 7000 series
- DINION HD 1080p
- DINION HD 1080p HDR
- DINION HD 720p
- DINION imager 9000 HD
- DINION IP bullet 4000
- DINION IP bullet 5000
- DINION IP 4000 HD
- DINION IP 5000 HD
- DINION IP 5000 MP
- DINION IP starlight 7000 HD
- FLEXIDOME corner 9000 MP
- FLEXIDOME HD 1080p
- FLEXIDOME HD 1080p HDR
- FLEXIDOME HD 720p
- Vandal-proof FLEXIDOME HD 1080p
- Vandal-proof FLEXIDOME HD 1080p HDR
- Vandal-proof FLEXIDOME HD 720p
- FLEXIDOME IP micro 2000 HD
- FLEXIDOME IP micro 2000 IP
- FLEXIDOME IP indoor 4000 HD
- FLEXIDOME IP indoor 4000 IR
- FLEXIDOME IP outdoor 4000 HD
- FLEXIDOME IP outdoor 4000 IR
- FLEXIDOME IP indoor 5000 HD
- FLEXIDOME IP indoor 5000 MP
- FLEXIDOME IP micro 5000 MP
- FLEXIDOME IP outdoor 5000 HD
- FLEXIDOME IP outdoor 5000 MP
- FLEXIDOME IP panoramic 5000
- IP bullet 4000 HD
- IP bullet 5000 HD
- IP micro 2000

- IP micro 2000 HD
- MIC IP dynamic 7000
- MIC IP starlight 7000
- TINYON IP 2000 family