1 Advisory Information

- **Advisory ID:** BOSCH-SA-033305-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-23849
    - Base Score: 7.5 (High)
- **Published:** 04 Aug 2021
- **Last Updated:** 07 Oct 2021

2 Summary

The possibility to conduct a CSRF (Cross Site Request Forgery) attack was discovered in a Penetration Test from Kaspersky ICS CERT during a certification effort from Bosch.

Bosch rates this vulnerability with CVSSv3.1 base scores of 7.5 (High), where the actual rating depends on the final rating specific to each customer's environment.

Customers are advised to upgrade to the fixed version or follow the described mitigation measures.

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

3 Affected Products

- Bosch CPP Firmware on: CPP4, CPP6, AVIOTEC, CPP7, CPP7.3, CPP13, CPP14

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the affected Bosch firmware to a fixed version. If an update is not available or possible in timely manner, users are recommended to follow the mitigation described in the following section.

Platform	Affected/revoked firmware	Fixed firmware
CPP4	7.10	n/a*
CPP6	7.60, 7.61	n/a*
	7.70, 7.80	7.81.0060
AVIOTEC	7.61, 7.72	7.81.0060
CPP7	7.60, 7.61	n/a*
	7.70, 7.72, 7.80	7.81.0060
CPP7.3	7.60, 7.61, 7.62	n/a*
	7.70, 7.72, 7.73, 7.80	7.81.0060
CPP13	7.75	8.10.0075
CPP14	8.00	8.20.0126

n/a* - A fix is currently not available. Please consider listed mitigation for a secure configuration environment.

4.2 Secure Configuration Environment

It is advised to use a Bosch tool like the Configuration Manager to configure the camera, that is not vulnerable to issues like XSS (Cross Site Scripting) or CSRF (Cross Site Request Forgery).

When using the web based configuration interface and currently being logged in as an administrator, some security precautions can be taken to mitigate XSS or CSRF vulnerabilities:

- No other websites or email content should be opened as long as the session to the camera is active.
- No links should be clicked from an untrusted external source that link back to the camera.
- Use a different browser than the system default browser to open a session to the camera as there is no XSS or CSRF between browsers.
- Always log out and/or close the browser (not only the tab) to clear any session data.

5 Vulnerability Details

5.1 CVE-2021-23849

CVE description: A vulnerability in the web-based interface allows an unauthenticated remote attacker to trigger actions on an affected system on behalf of another user (CSRF - Cross Site Request Forgery).

This requires the victim to be tricked into clicking a malicious link or opening a malicious website while being logged in into the camera.

- Problem Type:
  - CWE-352 Cross-Site Request Forgery (CSRF)
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 7.5 (High)

5.2 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] 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.

7 Revision History

- 07 Oct 2021: Update of fixed version
- 04 Aug 2021: Initial Publication

8 Appendix

8.1 Affected Plattforms and Cameras

CPP14

- FLEXIDOME multi 7000i

CPP13

- AUTODOME inteox 7000i
- MIC inteox 7100i

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