1 Advisory Information

- **Advisory ID:** BOSCH-SA-478243-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-23847
    - Base Score: 9.8 (Critical)
  - CVE-2021-23848
    - Base Score: 8.3 (High)
  - CVE-2021-23852
    - Base Score: 4.9 (Medium)
  - CVE-2021-23853
    - Base Score: 8.3 (High)
  - CVE-2021-23854
    - Base Score: 8.3 (High)
- **Published:** 09 Jun 2021
- **Last Updated:** 09 Jun 2021

2 Summary

Multiple vulnerabilities for Bosch IP cameras have been discovered in a Penetration Test from Kaspersky ICS CERT during a certification effort from Bosch.

Bosch rates these vulnerabilities with CVSSv3.1 base scores from 9.8 (Critical) to 4.9 (Medium), where the actual rating depends on the individual vulnerability and the final rating on the customer's environment.

Customers are strongly advised to upgrade to the fixed versions.

These vulnerabilities were discovered by Alexander Nochvay and Andrey Muravitsky from Kaspersky ICS CERT.

3 Affected Products

- Bosch CPP Firmware on: CPP4, CPP6, CPP7, CPP7.3, CPP13
  - CVE-2021-23848
  - CVE-2021-23852
  - CVE-2021-23853
- Bosch CPP Firmware 7.62 on: CPP6, CPP7, CPP7.3
  - CVE-2021-23854
- Bosch CPP Firmware 7.70 on: CPP6, CPP7, CPP7.3
  - CVE-2021-23847

- CVE-2021-23854
- Bosch CPP Firmware 7.72 on: CPP6, CPP7, CPP7.3
  - CVE-2021-23847
  - CVE-2021-23854
- Bosch CPP Firmware 7.75 on: CPP13
  - CVE-2021-23854
- Bosch CPP Firmware 7.76 on: CPP13
  - CVE-2021-23854
- Bosch CPP Firmware < 7.80 B128 on: CPP6, CPP7, CPP7.3
  - CVE-2021-23847

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 possible in timely manner, users are recommended to follow the mitigations and workarounds described in the following section.

Platform	Affected/revoked firmware	Fixed firmware
CPP4	7.10	7.10.0095
CPP6	7.60, 7.61	7.62.0005
	7.70, 7.80	7.80.0129
AVIOTEC	7.61, 7.72	7.72.0013
CPP7	7.60, 7.61	7.62.0005
	7.70, 7.72, 7.80	7.80.0129
CPP7.3	7.60, 7.61, 7.62	7.62.0005
	7.70, 7.72, 7.73, 7.80	7.80.0129
CPP13	7.75	7.75.0008

4.2 Firewalling

Disallowing connections from insecure networks to the camera by means of a firewall prevents the attacker from accessing the vulnerable interface.

4.3 IP Filtering

The camera has the possibility to whitelist networks or IP addresses to only allow access from trusted networks or IPs, preventing an attacker from accessing the camera.

4.4 Using certificate based authentication

To mitigate the critical vulnerability CVE-2021-23847, certificate based user authentication for the camera can be used as the SSL based authentication happens, before the vulnerable component can be accessed. This prevents an unauthenticated attacker from accessing the interface.

4.5 Secure Configuration Environment

It is advised to use a Bosch tool like the Configuration Manager to configure the camera, that does not allow for issues like XSS.

When using the web based configuration interface and currently being logged in as administrator, some security precautions can be taken to mitigate XSS 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 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-2021-23847

CVE description: A Missing Authentication in Critical Function in Bosch IP cameras allows an unauthenticated remote attacker to extract sensitive information or change settings of the camera by sending crafted requests to the device.

Only devices of the CPP6, CPP7 and CPP7.3 family with firmware 7.70, 7.72, and 7.80 prior to B128 are affected by this vulnerability. Versions 7.62 or lower and INTEOX cameras are not affected.

- Problem Type:
  - CWE-287 Improper Authentication
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

5.2 CVE-2021-23848

CVE description: An error in the URL handler may lead to a reflected cross site scripting (XSS) in the web-based interface. An attacker with knowledge of the camera address can send a crafted link to a user, which will execute javascript code in the context of the user.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
  - Base Score: 8.3 (High)

5.3 CVE-2021-23852

CVE description: An authenticated attacker with administrator rights can call an URL with an invalid parameter that causes the camera to become unresponsive for a few seconds and cause a Denial of Service (DoS).

- Problem Type:
  - CWE-400 Uncontrolled Resource Consumption
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 4.9 (Medium)

5.4 CVE-2021-23853

CVE description: Improper validation of the HTTP header allows an attacker to inject arbitrary HTTP headers through crafted URLs.

- Problem Type:
  - CWE-20 Improper Input Validation
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
  - Base Score: 8.3 (High)

5.5 CVE-2021-23854

CVE description: An error in the handling of a page parameter may lead to a reflected cross site scripting (XSS) in the web-based interface.

This issue only affects versions 7.7x and 7.6x. All other versions are not affected.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H
  - Base Score: 8.3 (High)

5.6 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

- 09 Jun 2021: Correction of build version number of fixed firmware
- 09 Jun 2021: Initial Publication

8 Appendix

8.1 Affected Plattforms and Cameras

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

- 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