1 Advisory Information

- **Advisory ID:** BOSCH-SA-844050-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2021-23863
    - Base Score: 6.1 (Medium)
- **Published:** 26 Jan 2022
- **Last Updated:** 07 Sep 2022

2 Summary

A vulnerability was recently discovered in the Android Application Bosch Video Security that allows an attacker to inject random HTML code into a WebView object. This vulnerability could for example allow the loading of malicious forms that could lead to the theft of the user's private information.

This vulnerability was discovered by Sergey Toshin of Oversecured.

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

Bosch rates this vulnerability using the CVSS 3.1 framework with a score of 6.1 (Medium).

3 Affected Products

- Bosch Video Security Android Application < 3.2.4

4 Solution and Mitigations

4.1 Software Updates

The recommended approach is to update the affected Bosch software to a fixed version. In this particular case, the user should verify that the Android Application is in the latest stable version, 3.2.4. This information can be consulted by accessing the Application settings menu.

4.2 Secure App Usage

The injection of random data into the Bosch Video Security App has to be triggered by a malicious 3rd party app on the same device. It is recommended to limit the installation of apps to well known good applications on critical devices.

© 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.

5 Vulnerability Details

5.1 CVE-2021-23863

CVE description: HTML code injection vulnerability in Android Application, Bosch Video Security, version 3.2.3. or earlier, when successfully exploited allows an attacker to inject random HTML code into a component loaded by WebView, thus allowing the Application to display web resources controlled by the attacker.

- Problem Type:
  - CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
  - Base Score: 6.1 (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] Google Play - Bosch Video Security: https://play.google.com/store/apps/details?id=com.bosch.onsite

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

8 Revision History

- 07 Sep 2022: Added mitigation measures
- 26 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.