



CYBERSECURITY ADVISORY

IMPROPER CERTIFICATE VALIDATION IN THE BTICINO DOOR ENTRY FOR HOMETOUCH ANDROID APPLICATION

Reference : LCA-2023-001

Date : 2023-06-02

Summary

Legrand is aware of a vulnerability in the Door Entry for HOMETOUCH Android application.

An attacker who successfully exploited this vulnerability could eavesdrops the communication between the mobile application and the cameras.

Affected products and versions

Product	Version
Door Entry for HOMETOUCH	All versions prior to 1.5.1

Vulnerability details

CVE ID	CVE-2022-46496
CVSS v3.1	Base Score 5.9 (Medium) – AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE	295 – IMPROPER CERTIFICATE VALIDATION

The application does not fully validate TLS certificates when connecting to www.myhomeweb.com. This vulnerability allows an attacker to perform a MitM attack, enabling them to capture user login credentials and SPI login / password information. This attack is particularly feasible in public or open Wi-Fi environment, making it relatively easy to execute.

Remediation

Legrand recommends installing the last version of the Android application at earliest convenience.

General security recommendations

We strongly recommend the following (non-exhaustive) cybersecurity best practices:

- Keep your smartphone and installed applications up to date in terms security patches.
- Remove all unused applications.

Acknowledgement

Legrand thanks Bruno Morisson for helping to identify the vulnerabilities and protecting our customers.

Support

For additional information please contact your Legrand local customer support. For contact information, see your country website (<https://www.legrand.com/>).

Legal disclaimer

The information provided in this security advisory is subject to change or update without notice and should not be construed as a commitment by Legrand.

This information is provided “as is” without any warranty or guarantee of any kind. The use of this security advisory is at the user’s own risk, and the user is solely liable for any damages to their systems or assets or other losses that may result from using this security advisory. Legrand disclaims all warranties relating to the information contained herein, whether express or implied, including the warranties of merchantability and fitness for a particular purpose. Under no circumstances shall Legrand or its suppliers be liable for any damages or losses of any nature or kind in connection with this security advisory and its use, including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Legrand or its suppliers have been advised of the possibility of such damages.

This document and parts thereof must not be reproduced or copied without written permission from Legrand. The contents hereof must not be shared with third parties nor used for any unauthorized purposes.