LEGRAND | BTICINO | NETATMO

EXPLOITING THE HARDWARE TO GAIN ACCESS TO THE WELCOME CAMERA

Reference : LCA-2019-001

Date : 2019-04-25

#LegrandImprovingLives

Summary

Legrand is aware of a vulnerability in the Netatmo Smart Indoor Camera product.

An attacker who successfully exploited this vulnerability could dump the firmware and forge a legitimate one, with new keys thanks to a uboot shell command, by physically accessing the device's serial port.

Affected products and versions

Product	Version
Smart Indoor Camera (formerly Welcome Camera)	All versions prior to 199

Vulnerability details

CVE ID	NA
CVSS v3.1	NA
CWE	NA

An attacker could exploit the vulnerability by physically accessing the camera's serial port. This will allow him to access the uboot shell, where he can retrieve the camera's firmware.

With access to the uboot shell, the attacker will be able to forge a new firmware signed with new keys thanks to the shell command, but also with the RSA key already present in the device.

Finally, the attacker could activate local SSH access by disabling Netatmo's SSH access.

Remediation

The security update has been installed automatically on the product.

General security recommendations

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

- Install physical controls so no unauthorized personnel can access your products.
- Connect products behind firewalls on networks separated from office or home networks.
- Minimize network exposure to prevent direct access from the Internet.
- Ensure all network components are always up to date in terms security patches.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

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.