CYBERSECURITY ADVISORY

LOCAL NETWORK REMOTE CODE EXECUTION ON SMART INDOOR CAMERA

Reference	:	LCA-2020-002
Date	:	2020-04-23

#Legrand**ImprovingLives**

legrand®

Summary

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

An attacker who successfully exploited this vulnerability could take control of the camera.

Affected products and versions

Product	Version
Smart Indoor Camera (formerly Welcome Camera)	All versions prior to 426

Vulnerability details

CVE ID	CVE-2019-17101
CVSS v3.1	Base Score 6.7 (Medium) – AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
CWE	77 – Improper Neutralization of Special Elements used in a Command ('Command Injection')

An attacker could exploit this vulnerability to gain elevated privileges manipulating the kernel memory management misleading the copy-on-write mechanism.

He could also exploit a script error in the device’s configuration to run an arbitrary code that could potentially take remote control on the product even pivoting on other devices of the same network.

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.

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.