LEGRAND | BTICINO | NETATMO

UNAUTHENTICATED ACCESS TO BUILT-IN REST API ON BTICINO MYHOMSERVER1

Reference : LCA-2022-001

Date : 2022-10-20

#LegrandImprovingLives

Summary

Legrand is aware of a vulnerability in the BTicino MYHOMESERVER1 product.

An attacker who successfully exploited this vulnerability could manipulate the configuration of the product.

Affected products and versions

Product	Version
MYHOMESERVER1	All versions prior to 2.60.34

Vulnerability details

CVE ID	NA
CVSS v3.1	Base Score 9.8 (High) – AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE	287 – Improper Authentication

Certain built-in REST API can be invoked without authentication (without JSESSIONID) both locally and remotely. Locally, this issue allows viewing and changing configuration by simply knowing the correct IP address and port. Remotely, by using the device's serial number on myhomeup.bticino.com website, one can obtain a bridge IP:TCP_PORT. This enables the use of the API to read and write configurations remotely.

By exploiting this vulnerability, from Internet, is possible to:

- Enumerate publicly accessible BTicino MYHOMESERVER1 installed systems
- Read rooms and configurations for enumerated systems
- Changing configuration of configured devices for enumerated systems (thermostats temperature settings, actuator settings).

Remediation

Legrand recommends installing the security update at earliest convenience. The steps and recommendations to install updates are described in the user manual.

Note: cloud services affected by this vulnerability have been discontinued.

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.