LEGRAND | BTICINO | NETATMO

MULTIPLE VULNERABILITIES IN MINKELS VARICONTROL

Reference : LCA-2025-001

Date : 2025-03-31

#LegrandImprovingLives

Summary

Legrand is aware of multiple vulnerabilities in the Minkels Varicontrol.

An attacker who successfully exploited this vulnerability could take remote control of the product and run arbitrary code.

Affected products and versions

Product	Version
Minkels Varicontrol	All versions prior to 406g

Vulnerability details

CVE ID	-
CVSS v3.1	Base Score 9.8 (Critical) - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE	78 and 306

Some vulnerabilities exist in the firmware included in the product versions listed above. An attacker could exploit these vulnerabilities by injecting unauthenticated system commands as parameters to the product management web server, enabling him to take control of the product.

Remediation

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

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.

Acknowledgement

Legrand thanks **Simon TULLING** 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.