Canon

Winbox Vulnerability

https://blog.mikrotik.com/security/winbox-vulnerability.html
https://nvd.nist.gov/vuln/detail/CVE-2018-14847 (awaiting analysis)

Overview:
Note: This Vulnerability represents our best knowledge as of the most recent revision. As a result, the content of this advisory is subject to change as further analysis is performed and the results are updated.

Canon Medical Systems USA, Inc., uses the Microtik RB450G for two products: 1) eProtect and 2) InnerVision (remote services) TVR. With 1) above, Canon Medical Systems is arranging a method to update the software and this advisory will be updated with further information.

In regards to 1) eProtect, all released software versions are V6.28 or earlier and is not applicable to the currently released information.

In regards to 2) InnerVision TVR, Canon Medical Systems uses a proprietary software control and this vulnerability is not applicable.

REFERENCE: https://securityaffairs.co/wordpress/75893/hacking/mikrotik-routers-hack.html

Possible Affected Canon Medical Systems USA, Inc. Products (investigating):
- None

Unaffected Products (investigating):
- InnerVision TVR's, eProtect

Resolution:
Canon Medical Systems USA, Inc. will update possible affected eProtect systems. In addition, Canon Medical Systems USA will update this advisory with instructions on how to update the software on MicroTik's eProtect devices when it becomes available.

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life

Notes:

Continue to check this advisory for updated information.

Please email CanonMedicalSystemsSecurity@us.medical.canon with any specific questions or issues.

Vulnerability Information:

- CVE-2018-14847

Advisory Change Log:

This is the first release of this Advisory

Release Date: 09/10/2018

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life