HMS Security Advisory Report

HMSSAR-2020-05-18-001

Publication date: 18 May 2020
Last update: 18 May 2020

Overview
TÜV Rheinland has informed HMS of a vulnerability concerning the verification process of some certificates.

Impact
Under certain conditions, an attacker might have been able to exploit this issue in an attempt to eavesdrop the connection with a forged certificate.

Affected products and versions
eCatcher before version 6.5.4

HMS Recommendations
Despite this issue, we remain confident in the security of our solution. Indeed, thanks to our “defense in depth approach” (https://ewon.biz/fr/a-propos/security/layered-security-approach), we use multiple mechanisms to validate the legality and authenticity of VPN tunnels before allowing forwarding of network traffic from and to this tunnel. We therefore tested our solution and confirm that eavesdropping of communications between Talk2M an eCatcher is not possible using this sole attack.

HMS recommends that eCatcher is updated to version >= 6.5.4 where the issue has been fixed.

Product updates
An update that completely fixes the problem is available here.

Acknowledgements
HMS thanks TÜV Rheinland for finding and notifying about the vulnerability in a controlled way.

Additional information
Ewon website vulnerability notification: https://www.hms-networks.com/cybersecurity