HMS Security Advisory Report

HMSSAR-2020-07-15-001

Publication date: 15 July 2020
Last update: 15 July 2020

Overview

Cybersecurity company Claroty has informed HMS of a vulnerability concerning the application eCatcher.

Impact

This vulnerability could be remotely exploited to gain remote code execution.

Affected products and versions

eCatcher before version 6.5.5

Severity / CVSS Score

The CVSS[1] severity base score is 9.6, and the associated scoring vector is

AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

HMS Recommendations

HMS recommends that eCatcher is updated to version >= 6.5.5 where the issue has been fixed.

Product updates

An update that fixes the problem is available here.

Acknowledgements

HMS thanks Claroty for finding and notifying about the vulnerability in a controlled way.

Additional information

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

[1] CVSS is owned by FIRST and used by permission. https://www.first.org/cvss

HMS Industrial Networks AB, PO Box 4126, 300 04 Halmstad, Sweden
Tel. +46 35 17 29 00, www.hms-networks.com