HMS Security Advisory Report

HMSSAR-2021-07-09-001

Publication date: 07 July 2021
Last update: 15 July 2021

Overview

Priyank Nigam from Bishop Fox reported to HMS Networks an Insecure Filesystem permissions in eCatcher prior to version 6.6.4. To exploit this vulnerability, an attacker must have a user account on the same machine than the victim (AV:L)(PR:L)(UI:R)(S:U) and have access to the machine during an active VPN connection (AC:L).

Impact

Weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files (I:L), or disruption of normal system operation (A:H). It was noted that the Talk2MVpnService service recreated this config file each time and prepended the filename with a random UUID which made it unpredictable. Hence, it was determined that the attack window was pretty small for exploitation which made a working exploit unreliable (C:L)

Affected products and versions

eCatcher - 6.6.4 and earlier

CVE Entry / CVSS Score

The CVE-2021-33214 with a CVSS\(^1\) severity base score of 6.1 has been assigned to this vulnerability, and the associated scoring vector is AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:H.

HMS Recommendations

HMS recommends that the software is updated to latest version (at least 6.7.3)

Product updates

Product update are available here: https://ewon.biz/technical-support/pages/alldownloads.

Acknowledgements

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

Additional information


---

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