HMS Security Advisory Report

HMSSAR-2020-09-11-001

Publication date: 11 September 2020
Last update: 11 September 2020

Overview

Parth Srivastava of Protiviti India Member Private Limited reported to HMS Networks a permissive Cross-domain Policy with Untrusted Domains in Ewon devices.

Impact

Affected devices use wildcards such as (*) under which domains can request resources. An attacker that has local access with high privileges could inject scripts into the Cross-origin Resource Sharing (CORS) configuration that could abuse this vulnerability, allowing the attacker to retrieve limited confidential information through sniffing.

Affected products and versions

Flexy and Cosy: All versions prior to firmware version 14.1.

CVE Entry / CVSS Score

The CVE-2020-16230 with a CVSS severity base score of 2.3 has been assigned (ICSA-20-254-03) to this vulnerability, and the associated scoring vector is AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N.

HMS Recommendations

HMS recommends that the products is updated to latest firmware version (from 14.1) in which xss filtering has been improved.

Product updates

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

Acknowledgements

HMS thanks Parth Srivastava 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