HMS information regarding BadAlloc, CVE-2020-15802

Overview of TIR-20210502

This report is an overview of a series of vulnerabilities discovered by Microsoft’s Section 52 research team, which they have labeled “BadAlloc”. More than 25 critical memory allocation vulnerabilities affecting various consumer, industrial, and medical IoT and OT devices have been identified. Successful exploitation of these vulnerabilities may give a malicious actor the ability to inject or execute remote code or cause the system to crash.

Referenced products

- Anybus Wireless Bridge II all variants
- Anybus Wireless Bolt Ethernet, Serial and CAN

HMS has investigated Anybus Wireless Bolt and Bridge and found that the vulnerability could not be exploited in these products.

HMS Recommendations

No action needed. HMS has investigated Anybus Wireless Bolt and Bridge and found that the vulnerabilities could not be exploited in these products.

Product updates

No action needed.

Additional information

Disclosure and listing of CVE’s can be found here:
https://www.avertium.com/blog/overview-badalloc-vulnerabilities