Baxter

Baxter Product Security Bulletin

RE: IPnet and VxWorks Urgent/11 Advisory

Publication Date: September 24, 2019
Update Date: October 21, 2019

SUMMARY

Baxter is currently monitoring the recently published ICS Advisory ICSA-19-211-01[1] and ICS Medical Advisory ICSMA-19-274-01[2]. Wind River and researchers from Armis reported 11 vulnerabilities (CVE-2019-12255 thru CVE-2019-12265) found in the Interpeak IPnet TCP/IP stack used in some versions of its real time operating system (RTOS) VxWorks. The vulnerabilities affect additional real time operating systems. The vulnerabilities have been classified as critical, high, and medium.

For a more detailed description of these vulnerabilities, it is recommended for customers to view the information provided by Wind River.[3]

RESPONSE

An initial assessment has been completed and it has been determined that no Baxter products use the IPnet TCP/IP stack or an impacted version of an RTOS. Baxter will continue to monitor all available information and we will provide an update to this bulletin if necessary.

---

[1] https://www.us-cert.gov/ics/advisories/icsa-19-211-01
[2] https://www.us-cert.gov/ics/advisories/icsma-19-274-01
[3] SECURITY ADVISORY: WIND RIVER TCP/IP STACK (IPNET) VULNERABILITIES
https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/security-advisory-ipnet/