المملكة العربية السعودية
الهيئة العامة للغذاء والدواء
Kingdom of Saudi Arabia
Saudi Food & Drug Authority

Medical Device Sector
Surveillance & Biometrics Executive Department

قطاع الأجهزة والمنتجات الطبية
الإدارة التنفيذية للرقابة والقياسات الحيوية

Safety Communication رسالة سلامة

Cybersecurity Vulnerabilities in a Third-Party Software Component (IPnet) May Introduce Risks During Use of Certain Medical Devices

Affected Operating Systems:	• VxWorks (by Wind River) • Operating System Embedded (OSE) (by ENEA) • INTEGRITY (by Green Hills) • ThreadX (by Microsoft) • ITRON (by TRON Forum) • ZebOS (by IP Infusion)
Problem:	Security researchers discovered 11 potentially serious security flaws, named "URGENT/11.", affecting some component of the above-mentioned operating systems. These vulnerabilities, which could lead to denial of service, information leaks, or logic errors, could affect variety of medical devices (such as imaging system, infusion pump, and anesthesia machine).
Recommendation/Actions:	1- Communicate your IT department to: a. Monitor the network traffic and logs for indications that an URGENT/11 exploit is taking place. b. Use firewalls, virtual private networks (VPN), or other technologies that minimize exposure to URGENT/11 exploitation. 2- Advise patients who use medical devices that may be affected. 3- Remind patients who use medical devices to seek medical help in case operation or function of their medical device changed unexpectedly. 4- Work with device manufacturers or legal authorized representatives within KSA to determine which medical devices in your facilities or in use by your patients could be affected by these vulnerabilities and develop risk mitigation plans. For more recommendations about Medical Devices Cybersecurity, Please refer to: (Guidance to Medical Devices Cybersecurity for Healthcare Providers) – MDS-G36