Title: Critical vulnerabilities in devices using VxWorks OS - URGENT/11
Advisory ID: CARESTREAM-2019-02
Issue Date: August 15, 2019
Last Revision Date: August 15, 2019
CVE(s): CVE-2019-12256, CVE-2019-12257, CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263, CVE-2019-12258, CVE-2019-12259, CVE-2019-12262, CVE-2019-12264, CVE-2019-12265

Are Carestream products vulnerable?

No currently supported Carestream products are affected by these vulnerabilities.

What is the URGENT/11 vulnerability?

The Armis research team, Armis Labs, have discovered 11 zero day vulnerabilities in VxWorks®, the most widely used operating system you may never heard about. VxWorks is used by over 2 billion devices including critical industrial, medical and enterprise devices. Dubbed "URGENT/11," the vulnerabilities reside in VxWorks' TCP/IP stack (IPnet), impacting all versions since version 6.5, and are a rare example of vulnerabilities found to affect the operating system over the last 13 years. Armis has worked closely with Wind River®, the maintainer of VxWorks, and the latest VxWorks 7 released on July 19 contains fixes for all the discovered vulnerabilities.

Six of the vulnerabilities are classified as critical and enable Remote Code Execution (RCE). The remaining vulnerabilities are classified as denial of service, information leaks or logical flaws. URGENT/11 is serious as it enables attackers to take over devices with no user interaction required, and even bypass perimeter security devices such as firewalls and NAT solutions. These devastating traits make these vulnerabilities 'wormable,' meaning they can be used to propagate malware into and within networks. Such an attack has a severe potential, resembling that of the EternalBlue vulnerability, used to spread the WannaCry malware.

For additional information on *the vulnerabilities please visit*: https://armis.com/urgent11/