



# Kentucky Hospital Research & Education Foundation Emergency Preparedness Update - 1 for July 30, 2019

[This information came in after the earlier Emergency Preparedness Update was distributed, and contains important information that you may want to forward to your IT Managers and Bio-medical Engineers.]

## Critical 'Update Now' Warning Issued For VxWorks OS Inside 2 Billion IoT Devices

(Forbes) -July 29 - A team of security researchers at California-based Armis has disclosed the discovery of 11 zero-day vulnerabilities in one of the world's most widely used IoT operating systems. VxWorks is so common, in fact, that it powers more than 2 billion devices around the world, including medical equipment, firewalls, elevators and industrial machinery. Armis describes VxWorks as "the most widely used operating system you have likely never heard about."

Armis has estimated that the vulnerabilities expose around 200 million of the devices carrying the VxWorks OS to the potential risk of attack. Six of the 11 vulnerabilities are critical, enabling Remote Code Execution (RCE). Vulnerabilities which open TCP/IP stacks to RCE attacks in this way are thankfully rare. The six critical (Remote Code Execution) vulnerabilities enable security layers to be bypassed and core systems to be attacked without any user response.

Here is a partial list of devices impacted from the [Armis Labs information](#):

- SCADA devices
- Industrial controllers
- Patient monitors
- MRI machines
- Firewalls
- VOIP phones
- Printers

As a part of their research, the Armis Labs team successfully exploited three devices using the URGENT/11 vulnerabilities in accordance with the attack scenarios identified. There are three video demonstrations in the [Armis Labs information](#).

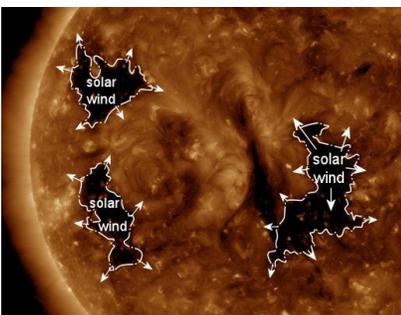
Full Forbes story: <https://www.forbes.com/sites/zakdoffman/2019/07/29/warning-as-2-billion-medical-industrial-and-enterprise-iot-devices-at-risk-of-attack/#5267815833af>

Detailed Armis Labs Briefing: <https://armis.com/urgent11/>

Wind River VxWorks statement: [https://blogs.windriver.com/wind\\_river\\_blog/2019/07/urgent-11-further-boosts-vxworks-security.html](https://blogs.windriver.com/wind_river_blog/2019/07/urgent-11-further-boosts-vxworks-security.html)

## Holes in the Sun's Atmosphere - Geomagnetic Unrest Possible

Earth is about to be strobed by three streams of solar wind--each flowing from a hole the sun's atmosphere. NASA's Solar Dynamics Observatory photographed the gaseous spigots on July 29th:



These are "coronal holes"--places where the sun's magnetic field peels back and allows solar wind to escape. Coronal holes look dark in extreme ultraviolet images of the sun because glowing-hot plasma normally contained there is missing.

The first of the streams is expected to arrive on **Aug 1st**, followed by two more in rapid succession on **Aug. 4th**. **Polar geomagnetic unrest and possibly some minor magnetic storms are possible on those dates.** *[See info below.]*

High-latitude sky watchers should be alert for auroras, especially in the southern hemisphere where winter darkness favors visibility.

Source: <http://www.spaceweather.com/>

Learn more - Wikipedia on Geomagnetic Storms: [https://en.wikipedia.org/wiki/Geomagnetic\\_storm](https://en.wikipedia.org/wiki/Geomagnetic_storm)

The KHREF Emergency Preparedness Update is assembled several times a week. When events make it necessary, the Update may be sent out several times a day to keep our hospital and the healthcare community advised on preparedness news and information. Most of this information is compiled from open sources, and where possible reference links will be provided. There is an archive of [Emergency Preparedness Updates available here](#). If you would like to added or deleted, or have something you would like to contribute to a future edition of the Emergency Preparedness Update, please contact [rbartlett@kyha.com](mailto:rbartlett@kyha.com) (include your current email address). The preparedness program for the Kentucky Hospital Association (KHA) and KHREF are supported by US DHHS ASPR HPP funds through a contract with Kentucky Public Health.