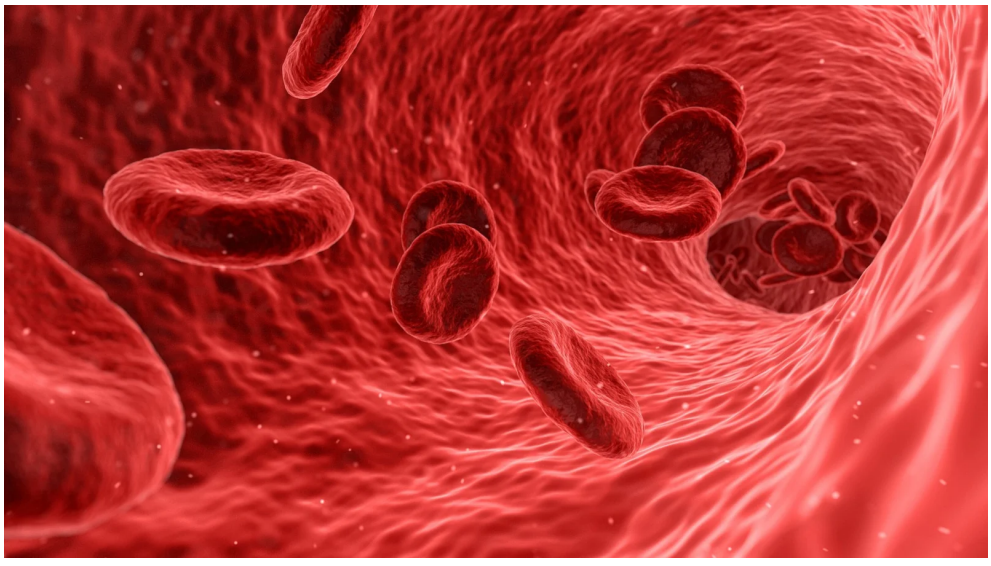
Over 100,000 medical infusion pumps vulnerable to years old critical bug

By
Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)

March 2, 2022 06:27 PM **0**

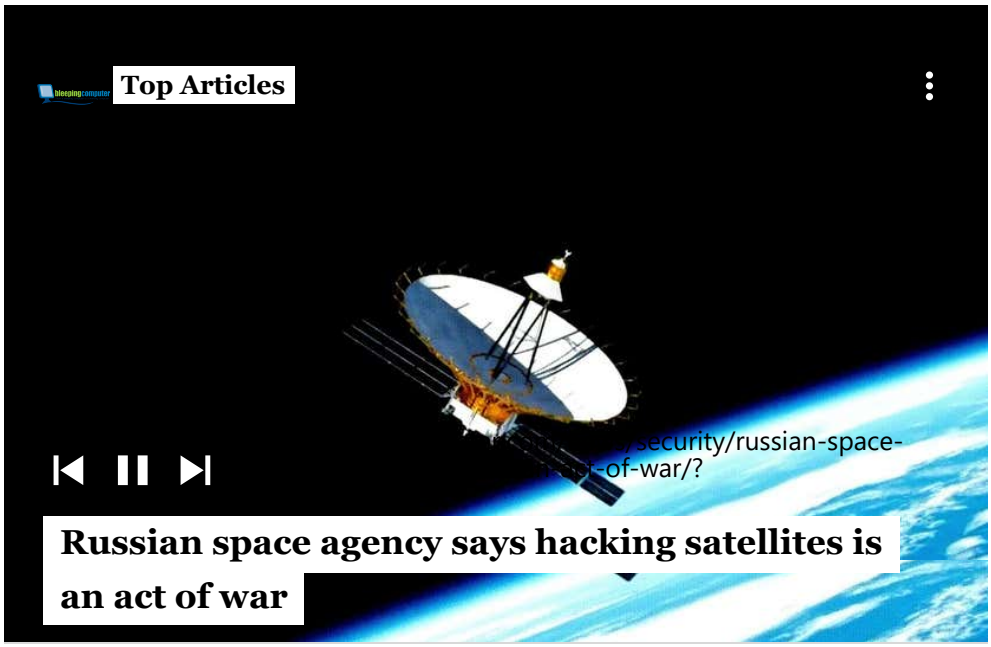


Data collected from more than 200,000 network-connected medical infusion pumps used to deliver medication and fluids to patients shows that 75% of them are running with known security issues that attackers could exploit.

The findings reveal that tens of thousands of devices are vulnerable to six critical-severity flaws (9.8 out of 10) reported in 2019 and 2020.

Old, critical issues persist

Using data collected from customers, researchers at Palo Alto Networks analyzed the security state of over 200,000 infusion pumps and found that between 30,000 and at least 100,000 of them are vulnerable to critical security issues.



The most prevalent critical-severity flaw encountered is CVE-2019-12255 (https://nvd.nist.gov/vuln/detail/CVE-2019-12255), a memory corruption bug in the VxWorks real-time operating system (RTOS) used for embedded devices, including infusion pump systems.

According to data from Palo Alto Networks, the flaw is present in 52% of the analyzed infusion pumps, which translates into more than 104,000 devices.

CVE-2019-12255 is part of a suite of 11 vulnerabilities known as 'URGENT/11 (https://www.bleepingcomputer.com/news/security/urgent-11-vxworks-rtos-vulnerabilities-found-critical-systems-affected/)' discovered and reported in 2019 by researchers at Armis, a company that provides security for connected devices.

Wind River, who maintains VxWorks RTOS, addressed all URGENT/11 issues in patches available since July 19, 2019. However, huge delays in applying updates or not installing them at all are well-known problems in the embedded device landscape.

The rest of five critical-severity bugs affect products from American health care company Baxter International and were reported in June 2020.

Critical-severity bugs in Baxter products and percentage of affected devices

identified by Palo Alto Networks IoT Security (https://www.paloaltonetworks.com/network-security/iot-security-for-healthcare)

	CVE	Severity (Score)	% of analyzed pumps with CVEs
1.	CVE-2020-12040 (https://nvd.nist.gov/vuln/detail/CVE-2020-12040)	9.8 (Critical)	17.83%
2.	CVE-2020-12047 (https://nvd.nist.gov/vuln/detail/CVE-2020-12047)	9.8 (Critical)	15.23%
3.	CVE-2020-12045 (https://nvd.nist.gov/vuln/detail/CVE-2020-12045)	9.8 (Critical)	15.23%
4.	CVE-2020-12043 (https://nvd.nist.gov/vuln/detail/CVE-2020-12043)	9.8 (Critical)	15.23%
5.	CVE-2020-12041 (https://nvd.nist.gov/vuln/detail/CVE-2020-12041)	9.8 (Critical)	15.23%

As per Baxter's security bulletin (https://www.baxter.com/sites/g/files/ebysai746/files/2020-06/ICSMA-20-170-04.pdf) at the time, exploiting most of them is possible if the actor is already on the network, which is far from being uncommon.

The bugs range from cleartext transmission of data without authentication to hardcoded credentials and incorrect permissions that allow access to sensitive data or changing the network configuration of the Wireless Battery Module.

No patches are available for these vulnerabilities but Baxter provided a set of mitigations (e.g. Segmentation, monitoring) designed to lower the risk of exploiting them and recommended switching to the newer Spectrum IQ Infusion system that is not affected by the issues above. An advisory (https://www.cisa.gov/uscert/ics/advisories/icsma-20-170-04) from CISA noted that a low-skilled attacker could exploit them.

In a post today, Palo Alto Networks recommends (https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/) healthcare providers adopt a proactive security strategy for keeping devices safe from known and unknown threats, which starts with an accurate inventory of all systems on the network.

The researchers note that not all the vulnerabilities currently affecting the analyzed infusion pumps are practical for remote attacks but they are a "risk to the general security of healthcare organizations and the safety of patients."

Related Articles:

Microsoft Exchange servers hacked to deploy Cuba ransomware (https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/)

Microsoft fixes actively exploited Exchange zero-day bugs, patch now (https://www.bleepingcomputer.com/news/security/microsoft-fixes-actively-exploited-exchange-zero-day-bugs-patch-now/)

CISA compiles list of free cybersecurity tools and services (https://www.bleepingcomputer.com/news/security/cisa-compiles-list-of-free-cybersecurity-tools-and-services/)

WordPress force installs UpdraftPlus patch on 3 million sites (https://www.bleepingcomputer.com/news/security/wordpress-force-installs-updraftplus-patch-on-3-million-sites/)

Hackers can crash Cisco Secure Email gateways using malicious emails (https://www.bleepingcomputer.com/news/security/hackers-can-crash-cisco-secure-email-gateways-using-malicious-emails/)