DARKMATTER

DARKMATTER ADVISORY – URGENT/11

05 AUGUST 2019

SMART AND SAFE DIGITAL

Executive Summary

Eleven critical vulnerabilities in VxWorks (the most widely used real-time operating system) have been made public.

Impacted Systems: VxWorks 6.5 and above, excluding the certification version and the latest version, are impacted.

Risk: Significant risk as these vulnerabilities could allow remote code execution without any human intervention.

CVSS Severity Score: 9.8 / 10 (Critical Rating)

DarkMatter Recommendations: Upgrade to the latest version and /or deploy patches for the current version.

Overview

VxWorks, from Wind River, is the most widely deployed real-time operating system that is used across industries such as aerospace, defense, medical devices, industrial equipment, energy, network infrastructure and consumer electronics. World-wide, this operating system is used by over 2 billion devices and its TCP/IP stack is used by many other vendors.

On 29th of July 2019, the Armis research team made public eleven vulnerabilities affecting VxWorks operating system. Dubbed "Urgent/11" these vulnerabilities impact the TCP / IP stack of the operating system and pose a significant security risk to the devices running VxWorks.

Technical Details

In a paper released by Armis Labs, eleven vulnerabilities impacting the TCP / IP stack of VxWorks were identified. Of these, six vulnerabilities are critical and can lead to Remote Code Execution. The remaining vulnerabilities are classified as denial of service, information leakage or logical flaws.

These vulnerabilities could allow an attacker to take over these devices with no user interaction required. These can even bypass perimeter security devices like firewalls and NAT solutions. As a result, these are similar to the EternalBlue vulnerability that led to the Wannacry outbreak.

All versions of VxWorks 6.5 and above or devices that leverage the VxWorks TCP/IP stack are impacted by one or more of the Urgent/11 vulnerabilities. VxWorks versions designed for certification (VxWorks 653 and VxWorks Cert Edition) and the latest version (VxWorks 7 SR620) are not impacted.

Mitigations

Unless organizations proactively and promptly mitigate the risk, the implications could be severe. Potential scenarios range from complete takeover of the devices to shutting down critical systems.

DarkMatter provides the following recommendations for organizations impacted by these vulnerabilities. The latest version of VxWorks is not impacted by these vulnerabilities. Where possible organizations should upgrade to the latest version. Wind River has also produced controls and patches to mitigate the reported vulnerabilities. Organizations should email PSIRT@windriver.com and obtain the required patches.

Lastly, organizations should take note of the Wind River advisory that provides additional general remediations that may allow mitigation of some of the vulnerabilities.

In addition, a number of other vendors have released advisories for their products impacted by these vulnerabilities. We strongly advise organizations to check those advisories at:

SonicWall: https://blog.sonicwall.com/en-us/2019/07/wind-river-vxworks-and-urgent-11-patch-now/

Rockwell Automation: https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1088561

Xerox: https://security.business.xerox.com/en-us/news/wind-river-vxworks-ipnet-tcp-ip-stack-vulnerabilities/

ABB:
http://search-ext.abb.com/library/Download.aspx?DocumentID=8VZZ001892T0001&LanguageCode=en&DocumentPartId=&Action=Launch

DarkMatter MSS Customers

Our MSS team is optimizing the signatures for various monitoring platforms and our MSS customers will be alerted should we notice any suspicious activity on their network.

Contact Us

Should you need additional details, you can reach out to us at contactus@darkmatter.ae.