WOODWARD

Security Bulletin **01661A**
(8/2019)

VxWorks Urgent/11 Vulnerabilities

Issue

Wind River, the developer of the VxWorks RTOS (Real-Time Operating System) ("VxWorks") identified a set of vulnerabilities, known as "Urgent/11," in the network stack (IPnet) within the VxWorks Operating Software versions 6.5 and later. This security bulletin addresses mitigation of certain vulnerabilities through the use of external firewalls in the Woodward Products identified below (the "Affected Units"). Woodward will integrate and deploy patches issued by Wind River for additional vulnerabilities through the release of product-specific Security Bulletins and security patches.

Description

A specially crafted network packet using the TCP Urgent Pointer flag may highjack an existing TCP session and inject bad TCP-segments, or establish a new TCP-session on a port the victim system listens to. This may lead to a crash in the application, loss of communication with the control or a potential remote code execution (RCE).

This bulletin addresses the following CVE's:

CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263

CVE's that will be addressed in future bulletins:

CVE-2019-12256, CVE-2019-12257, CVE-2019-12258, CVE-2019-12262, CVE-2019-12264, CVE-2019-12259, CVE-2019-12265

Affected Units

MicroNet Plus and TMR: 5466-1045, 5466-1047, 5466-1141, 5466-1145, 5466-1245, 5466-1247, 5466-1250, 5466-1347, 5466-1510, 5466-1520

Flex500/505D/505XT/Vertex/Peak200: 8200-1300, 8200-1301, 8200-1302, 8200-1310, 8200-1311, 8200-1312, 8200-1340, 8200-1341, 8200-1342, 8200-1350, 8200-1351, 8200-1352, 8200-1360, 8200-1370, 8200-1371, 8200-1500, 8200-1501, 8200-1502, 8200-1503, 8200-1504, 8200-1505, 8200-1508, 8200-1509

Atlas II / Intelligent Gateway: 8273-587, 8273-700

Please note that these controls may be components in systems or cabinet assemblies manufactured by the turbine OEM, Woodward or Woodward Channel Partners

Corrective Action

For applications where devices reside behind a network firewall, the four "TCP Urgent Pointer" vulnerabilities can be mitigated via the firewall. IT administrators can add a rule to drop/block any TCP-segment where the URG-flag is set. The "Urgent data" feature is used by very few applications. It had some uses in the early days of the Internet when used with serial terminals. It is not used by modern applications such as HTTP, SSH, SSL/TLS, etc.

If no network or other external firewall is present, Woodward recommends that the site implement a defense in depth strategy that includes an external firewall to filter traffic to the control.

Additional Information

ICS Advisory 19-211-01: https://www.us-cert.gov/ics/advisories/icsa-19-211-01

Wind River Security Advisory: https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/security-advisory-ipnet/

WOODWARD

PO Box 1519, Fort Collins CO 80522-1519, USA
1041 Woodward Way, Fort Collins CO 80524, USA
Phone +1 (970) 482-5811

Email and Website—www.woodward.com

Woodward has company-owned plants, subsidiaries, and branches, as well as authorized distributors and other authorized service and sales facilities throughout the world.

Complete address / phone / fax / email information for all locations is available on our website.