

Urgent/11 Patch – MicroNet Cyber-Ready 5200CPU

Issue

As announced in August (see Security Bulletin 01661), a set of vulnerabilities known as “Urgent/11” were discovered in the network stack (IPnet) within the Wind River VxWorks Real-Time Operating Software versions 6.5 and later which are used on the MicroNet Plus Cybersecure 5200 CPUs.

Woodward has integrated patches provided by Wind River into the 5200 CPU Footprint software and is now in the final stages of verification testing. This security bulletin addresses how to patch the Cyber-Ready CPU (the “Affected Unit”). These patches will be made available on Woodward.com by October 7, 2019.

Description

The necessary Service Pack can be downloaded from the Woodward website.

The patches described in this bulletin addresses the following vulnerabilities:

CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263 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: 5466-1045 Cyber-Ready CPU

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

Corrective Action

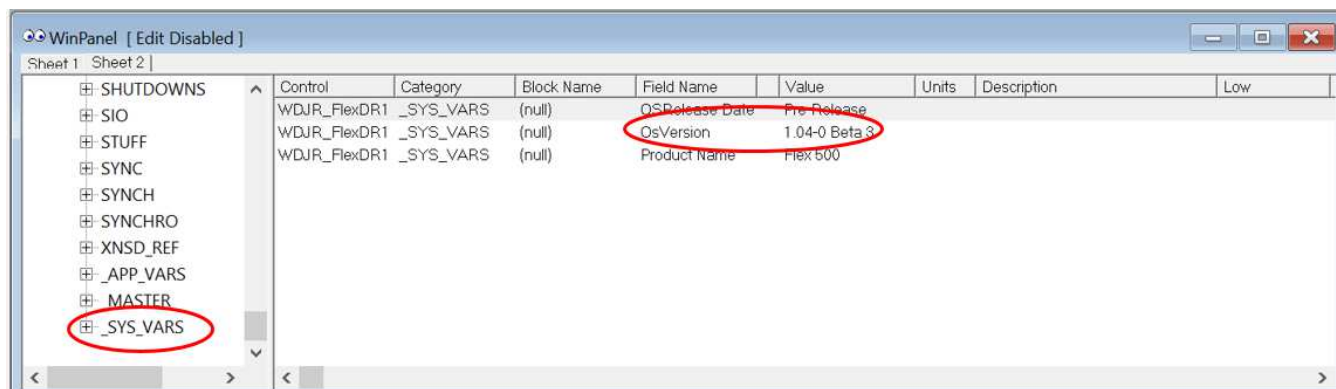
A patch is not available for the version of VxWorks used on the 5466-1045 “Cyber Ready” CPU. For this reason, Woodward is providing customers currently running this CPU with a free upgrade to the 5466-1145 Cyber Secure CPU. There are two system configurations that must be verified prior to installing the patch upgrade:

1. The majority of 5466-1045 CPUS are installed in systems running on Coder 6.00-4 or later and do not require any change to the GAP Application software, however a few may be running older Coders that require an Application software update.
2. Some 5466-1045 Cyber-ready CPUs were not licensed for Cybersecurity. This must be checked and the Cybersecurity upgrade installed if necessary. This upgrade will be provided free of charge by Woodward.

It is necessary to verify these items before installing the Service Packs.

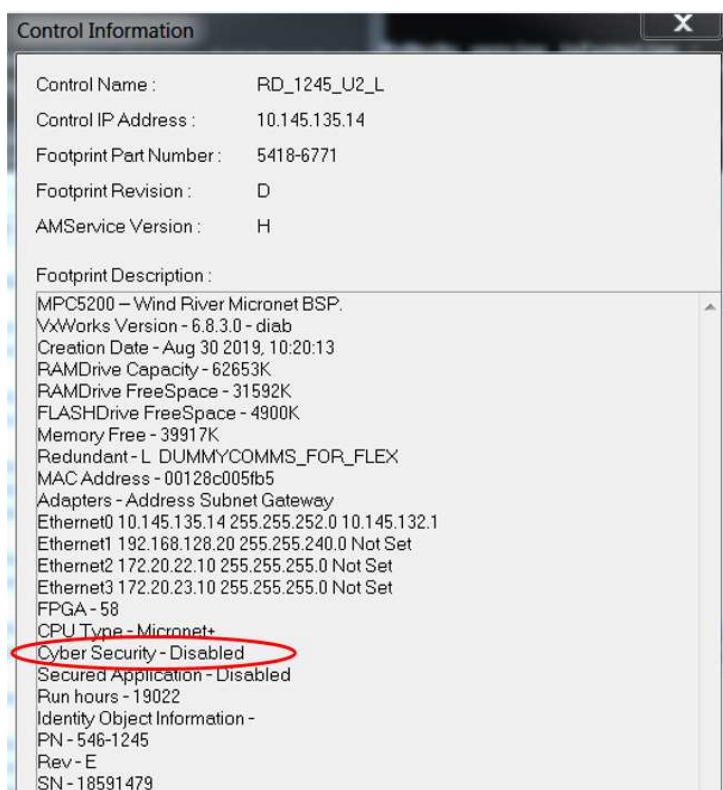
First, determine the Coder version on your system:

- Use Woodward Control Assistant and look at _SYS_VARS to determine the Coder version. This can be done with the turbine running. See the example below:
- Coder shows as OsVersion under _SYS_VARS in Control Assistant. On the example below, the system is running Coder 1.04-0:



- If the system is running Coder 6.00-4 or later, or any revision of Coder 1.00, 1.01, 1.02, etc. it will work with this upgrade.
- If the system is running an older Coder (5.04 to 6.00-3), it will be necessary to recompile the application with a new Coder prior to upgrading. Please stop and request assistance from your system support resource (the turbine OEM, Woodward or a Woodward partner).
- If you have Coder 6.00-4 or later, determine if Cyber Security is enabled on your CPU.

Use the Control Information screen in AppManager to see if the CPU has Cyber Security enabled. This example shows a CPU with Cyber Security is disabled.



If the screen shows "Disabled" please contact Woodward with your CPU serial number(s) and a site code will be provided to enable Cybersecurity on the CPUs. Use AppManager to install the applicable site code on each CPU in the system.

When Cyber Security is enabled, you will have User Account Management and secure passwords available on your system.

Once you have confirmed the Coder version you are running and that the system has Cyber Security enabled, please proceed as follows to install the upgrade service packs:

Service Packs are installed by connecting AppManager to the CPU (in redundant systems, use the Syscon CPU which is normally the left CPU). Woodward recommends using AppManager version 3.14 or later to install the upgrades. AppManager can be downloaded from the Woodward website.

CPU Upgrade (after confirming Coder version and that Cyber Security is enabled):

The CPUs are upgraded by sequentially installing two service packs:

1. Service Pack 9927-2346 is installed first
2. Service Pack 9927-2721 is installed second

The RTN network used to communicate with Woodward expansion chassis or RTN Gateways is not affected by the Urgent 11 vulnerabilities, however if your system uses expansion chassis you may wish to upgrade the RTN modules using the same twostep process described above. Each CPU and RTN module can be seen and upgraded using AppManager.

Further instructions on installing the above Service Packs is available within AppManager. Most sites should be able to install Service Packs without assistance, however if you are not comfortable doing this, please contact your support resource (turbine OEM, Woodward or Woodward partner) for assistance.

Your support resource can also log the upgrade into Woodward's system so that our serial number records are correctly updated. Woodward can provide you with an updated nameplate if desired.

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/>

**Copyright © Woodward, Inc. 2019
All Rights Reserved**



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.