CYBER SECURITY NOTIFICATION

Cyber Security Notification

Wind River Advanced Security Notice - VxWorks TCP/IP stack

Update date: None (original document)

Notice

Affected Products

AC 800PEC embedded software releases 5.1.0.0 and later. This means, all ABB products that use the 3rd generation of the AC 800PEC controller are potentially affected.

Summary

Wind River is the provider of the real time operating system VxWorks 6.8.3 which is used in the embedded software of the AC 800PEC controller.

Windriver has recently become aware of security vulnerabilities in the Wind River TCP/IP stack (IPnet) which is used in the AC 800PEC. This means that all Ethernet based protocols are affected. In certain scenarios this would lead to the controller becoming inaccessible.

The vulnerabilities do not target any ABB products specifically, but potentially affect products that use the AC 800PEC controller.

Wind River is working on the patch which will be provided to the AC 800PEC team in the next few weeks. As soon as the patch is applied, implemented and tested, we will inform our internal customers about the available bug fix version.

The Wind River vulnerability CVE numbers and titles are listed in the table below:

CVE	Title	CVSSv3 Score
CVE-2019-12256	Stack overflow in the parsing of IPv4 packets' IP options	9.8
CVE-2019-12257	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc	8.8
CVE-2019-12255	TCP Urgent Pointer = 0 leads to integer underflow	9.8
CVE-2019-12260	TCP Urgent Pointer state confusion caused by malformed TCP AO option	9.8
CVE-2019-12261	TCP Urgent Pointer state confusion during connect() to a remote host	8.8
CVE-2019-12263	TCP Urgent Pointer state confusion due to race condition	8.1
CVE-2019-12258	DoS of TCP connection via malformed TCP options	7.5
CVE-2019-12259	DoS via NULL dereference in IGMP parsing	6.3
CVE-2019-12262	Handling of unsolicited Reverse ARP replies (Logical Flaw)	7.1
CVE-2019-12264	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client	7.1
CVE-2019-12265	IGMP Information leak via IGMPv3 specific membership report	5.4

Recommended immediate actions

Recommended security practices and firewall configurations can help protect the AC 800PEC controller from attacks that originate from outside the network.

Additional recommendations:

- Use the AC 800PEC within a secure network
- Add a firewall in the network. Administrators can add a rule to drop/block any TCP-segment where URG-flag is set.

Support

For additional information and support please contact your local ABB service organization. For contact information, see http://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

For AC 800PEC specific questions please get in contact with the AC 800PEC team (pec@ch.abb.com) .