# ICS-CERT ADVISORY

## ICSA-10-214-01— VXWORKS VULNERABILITIES

August 2, 2010

## OVERVIEW

A security researcher has identified two vulnerabilities affecting the Wind River Systems' VxWorks platform. The vulnerabilities are a debug service enabled by default (VU#362332[a]) and a weak hashing algorithm used in authentication (VU#840249[b]). ICS-CERT has been coordinating with CERT/CC in alerting control systems vendors of these vulnerabilities. ICS-CERT will continue to coordinate and publish updates as needed.

## AFFECTED PRODUCTS

VxWorks is a real-time operating system that can be used in embedded systems, including control system components. Because this vulnerability is embedded in other products, the actual list of affected products is large, and not completely known.

Not all products using VxWorks are vulnerable. ICS-CERT recommends that end users contact their vendors to determine if their products are affected by these vulnerabilities. CERT/CC has a partial list of vendors in the Vulnerability Notes referenced above.

## IMPACT

Access to the debug service could result in information disclosure or denial-of-service attacks against the affected device. Complete control of the device may be possible.

The authentication vulnerability could allow an attacker to guess the password and gain unauthorized access to the device.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their environment, architecture, and product implementation.

a. Vulnerability Note, http://www.kb.cert.org/vuls/id/362332.
b. Vulnerability Note, http://www.kb.cert.org/vuls/id/840249.

## BACKGROUND

VxWorks is a trademark of Wind River Systems. VxWorks has been used in more than 500 million deployed devices,[c] ranging from aerospace and defense applications to networking and consumer electronics, robotics and industrial applications, precision medical instruments, and car navigation and telematics systems.[d]

# VULNERABILITY CHARACTERIZATION

## VULNERABILITY OVERVIEW

The following two vulnerabilities have been identified:

1. Debug Service Enabled by Default – Some products based on VxWorks ship with the debug service enabled on UDP port 17185. This service provides read and write access to the device's memory and allows functions to be called. An attacker could use this service to fully compromise the device.

   The overall Common Vulnerability Scoring System (CVSS) severity score[e] for this vulnerability is 8.6 (high). The following link provides a calculator for viewing details of the score: http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:W/RC:C)

2. Weak Hashing Algorithm – The standard VxWorks authentication API uses a weak password hashing algorithm. This algorithm produces a small set of outputs for a large set of inputs, resulting in multiple strings having the same hash, otherwise known as collisions. An attacker could brute force the password in a relatively short period of time by guessing a string that produces the same hash as the legitimate password.

   The overall CVSS severity score for this vulnerability is 7.7 (high). The following link provides a calculator for viewing details of the score: http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:C/I:C/A:C/E:POC/RL:W/RC:C)

c. http://www.windriver.com/products/vxworks, website last accessed July 29, 2010.
d. http://www.windriver.com/products/product-overviews/PO_VE_3_8_Platform_1209.pdf.
e. http://nvd.nist.gov/cvss.cfm?calculator&version=2.

## VULNERABILITY DETAILS

### EXPLOITABILITY

The enabled debug service allows full access to the memory of the device to an unauthenticated remote user. A memory dump would likely reveal passwords and configuration information. An attacker could use write access to perform denial-of-service attacks, and if familiar with the device, could gain complete control.

Exploiting the vulnerability in the authentication API would require the following:

- The default API must be the authentication method used
- The attacker would first need a valid username
- The attacker would need access to a service using the API such as rlogin, Telnet or FTP.

### EXISTENCE OF EXPLOIT

Proof-of-concept code is expected to be made public by the researcher. However, at the time of this writing, no known exploits exist in the field specifically targeting these vulnerabilities.

### DIFFICULTY

Accessing the debug service would be trivial unless blocked by a firewall. An attacker may need to be familiar with the device to control it by writing to memory; however, a memory dump would not be difficult.

Brute forcing a password is not difficult, and software tools exist to automate the process. Exploiting the authentication API vulnerability is made easier by the fact that no account lockout is implemented by default. Users are not disconnected for too many incorrect login attempts.

## MITIGATION

The mitigations differ for vendors utilizing VxWorks in their products, and the end-users of these products.

## VENDORS USING VXWORKS

Vendors using VxWorks in their products should disable the debug agent for production systems. The VxWorks Kernel Programmer's 6.8 Guide recommends that only those components needed for deployed operation be enabled. Components required for host development support such as the debug agent and debugging components should be removed.

Vendors should not use the standard default authentication API (loginDefaultEncrypt()) in their VxWorks products. Other encryption routines can be implemented by using the loginEncryptInstall() routine in the

VxWorks loginLib library. Contact Wind River Support[f] or refer to Vulnerability Note VU#840249[g] for instructions. A trusted authentication API should be chosen to replace the standard default.

## USERS OF PRODUCTS WITH EMBEDDED VXWORKS

End users should restrict access to debug port 17185/udp with appropriate firewall rules. It is good security practice to block all ports not explicitly needed for operation. This is referred to as a "default deny" policy.

Users should restrict access to any service that uses the standard default authentication (e.g., rlogin, Telnet, FTP) with appropriate firewall rules. If possible, such services should be disabled if not needed. Intrusion detection/prevention systems can be used to detect brute force attacks (password guessing) against such services.

The Control System Security Program also provides a recommended practices section[h] for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

f. http://www.windriver.com/support/.

g. Vulnerability Note, http://www.kb.cert.org/vuls/id/840249.

h. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 12, 2010.

## CONTACT ICS-CERT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For Control System Security Program Information and Incident Reporting:
www.ics-cert.org

## DOCUMENT FAQ

***What is an ICS-CERT Advisory?*** An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

***Can I edit this document to include additional information?*** This document may not be edited or modified in any way by recipients nor may any markings be removed. All comments or questions related to this document should be directed to the ICS-CERT at ics-cert@dhs.gov.