ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-091-01, WIND RIVER VXWORKS SSH AND WEB SERVER MULTIPLE VULNERABILITIES

April 01, 2013

OVERVIEW

This advisory provides mitigation details for multiple vulnerabilities in the Wind River VxWorks Remote Terminal Operating System (RTOS).

Hisashi Kojima and Masahiro Nakada of Fujitsu Laboratories have reported six vulnerabilities in Wind River's VxWorks SSH and Web Server. Successful exploitation of these vulnerabilities could cause a denial-of-service (DoS) condition in the RTOS. One of these vulnerabilities could allow remote code execution if exploited. These vulnerabilities were originally reported to JPCERT/CC. Wind River has produced patches that mitigate these vulnerabilities. These vulnerabilities affect devices using VxWorks in the critical manufacturing, energy, and water and wastewater sectors.

These vulnerabilities can be exploited remotely.

AFFECTED PRODUCTS

The following Wind River products are affected:

- Web Server & CLI vulnerabilities: VxWorks Versions 5.5 through 6.9, and
- SSH vulnerabilities: VxWorks Versions 6.5 through 6.9.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

IMPACT

Exploitation of each of these vulnerabilities can cause VxWorks to be unavailable until the next reboot.

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 operational environment, architecture, and product implementation.

BACKGROUND

Wind River is a US-based company that sells products around the world. Wind River is a wholly owned subsidiary of Intel Corporation.

The affected product, VxWorks, is a real time operating system. VxWorks and other RTOS are used within industrial control systems made by many different manufactures. Wind River VxWorks is deployed across several sectors including critical manufacturing, energy, water and wastewater, and others. Wind River estimates that these products are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER INPUT VALIDATION[a]

The SSH server (IPSSH) implementation in VxWorks 6.5 through 6.9 contains a DoS vulnerability due to an issue in processing authentication requests.[b] An attacker could send specially crafted authentication requests that cause SSH server outage. SSH access may become unavailable until the next reboot as a result of this vulnerability being exploited.

CVE-2013-0711[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C). [d]

a. CWE-20: Improper Input Validation, http://cwe.mitre.org/data/definitions/20.html, Web site last accessed April 01, 2013.
b. JVNDB-2013-000018, http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000018.html, Web site last accessed April 01, 2013.
c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0711 , Web site last accessed April 01, 2013.
d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited April 01, 2013.

IMPROPER INPUT VALIDATION[a]

The SSH server (IPSSH) implementation in VxWorks 6.5 through 6.9 contains a DoS vulnerability due to an issue in the processing directly after the SSH connection is established.[e] Successful exploitation of this vulnerability may cause SSH access to become unavailable until the next reboot. An attacker could send specially crafted packets that cause SSH server outage. The attacker must login with a valid user name and password combination before launching a successful attack.

CVE-2013-0712[f] has been assigned to this vulnerability. A CVSS v2 base score of 6.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:N/I:N/A:C). [g]

IMPROPER INPUT VALIDATION[a]

The SSH server (IPSSH) implementation in VxWorks 6.5 through 6.9 contains a DoS vulnerability due to an issue in processing pty requests.[h] Receiving a specially crafted pty request packet may cause SSH access to be unavailable until the next reboot. The attacker must login with a valid user name and password combination before launching a successful attack.

CVE-2013-0713[i] has been assigned to this vulnerability. A CVSS v2 base score of 6.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:N/I:N/A:C). [j]

IMPROPER INPUT VALIDATION[a]

The SSH server (IPSSH) implementation in VxWorks 6.5 through 6.9 contains vulnerability due to an issue in the processing authentication requests.[k] Receiving a specially crafted packet for a public key authentication request may cause the server to hang and SSH access to be unavailable

e. JVNDB-2013-000019 - VxWorks SSH server (IPSSH) denial-of-service (DoS) vulnerability, http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000019.html , Web site last accessed April 01, 2013.

f. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0712, Web site last accessed April 01, 2013.

g. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:N/I:N/A:C), Web site last accessed April 01, 2013.

h. JVNDB-2013-000020 - VxWorks SSH server (IPSSH) denial-of-service (DoS) vulnerability, http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000020.html, Web site last accessed April 01, 2013.

i. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0713, Web site last accessed April 01, 2013.

j. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:N/I:N/A:C), Web site last accessed April 01, 2013.

k. JVNDB-2013-000021 - VxWorks SSH server (IPSSH) denial-of-service (DoS) vulnerability, http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000021.html, Web site last accessed April 01, 2013.

until the next reboot. In addition, arbitrary code may be executed on the server with administrator privileges.

CVE-2013-0714[l] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C). [m]

COMMAND INJECTION[n]

The WebCLI component in VxWorks 5.5 through 6.9 contains a DoS vulnerability due to an issue in parsing command strings.[o] An attacker that can login to a CLI session may cause the current CLI session to terminate. A new CLI session may be re-established without rebooting.

CVE-2013-0715[p] has been assigned to this vulnerability. A CVSS v2 base score of 6.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:N/I:N/A:C).[q]

IMPROPER INPUT VALIDATION[a]

The Web Server in VxWorks 5.5 through 6.9 contains a DoS vulnerability.[r] When a user accesses the VxWorks Web Server using a specially crafted URL, the server may crash.

CVE-2013-0716[s] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:P).[t]

l. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0714, Web site last accessed April 01, 2013.
m. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=%20(AV:N/AC:L/Au:N/C:N/I:P/A:C), Web site last accessed April 01, 2013.
n. CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), http://cwe.mitre.org/data/definitions/78.html, Web site last accessed April 01, 2013.
o. JVNDB-2013-000022 - VxWorks WebCLI vulnerable to denial-of-service (DoS), http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000022.html, Web site last accessed April 01, 2013.
p. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0715, Web site last accessed April 01, 2013.
q. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector= (AV:N/AC:L/Au:S/C:N/I:N/A:C), Web site last accessed April 01, 2013.
r. JVNDB-2013-000023 - VxWorks WebCLI vulnerable to denial-of-service (DoS), http://jvndb.jvn.jp/en/contents/2013/JVNDB-2013-000023.html, Web site last accessed April 01, 2013.
s. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0716, Web site last accessed April 01, 2013.
t. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector= (AV:N/AC:L/Au:N/C:N/I:N/A:P), Web site last accessed April 01, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities.

MITIGATION

According to Wind River, software patches for these vulnerabilities are available for all affected VxWorks versions. Users interested in obtaining these patches should contact Wind River technical support for assistance: http://windriver.com/support/

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[u] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion

u. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed April 01, 2013.

Detection and Mitigation Strategies,[v] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

v. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed April 01, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

I see that this document is labeled as TLP = WHITE. May I distribute this to other people?
According to the International Critical Information Infrastructure Protection (CIIP) Traffic Light Protocol[w,x] warning, this document is subject to standard copyright rule and may be distributed freely without restriction.

TLP = WHITE: Unlimited

w. Traffic Light Protocol—International CIIP Directory, Issue 21, September 2009.
x. US-CERT, http://www.us-cert.gov/tlp/, Web site last accessed April 01, 2013.