ICS-CERT ADVISORY

ICSA-12-263-02—ORING INDUSTRIAL NETWORKING IDS-5042/5042+ HARD-CODED CREDENTIAL VULNERABILITY

September 19, 2012

OVERVIEW

Independent researcher Reid Wightman of Digital Bond[a] identified hard-coded credentials in the operating system of the ORing Industrial DIN-Rail Device Server 5042/5042+ systems and publicly released this information without coordination with ICS-CERT, the vendor, or any other coordinating entity known to ICS-CERT. This vulnerability grants attackers administrative access to the device. ICS-CERT has been unable to successfully coordinate this vulnerability with ORing Industrial Networking because of the vendor's unresponsiveness. ICS-CERT is unaware of any fix by ORing Industrial Networking that mitigates this vulnerability.

This vulnerability can be exploited remotely. Exploits that target this vulnerability are known to be publicly available.

AFFECTED PRODUCTS

The following ORing Industrial Networking products are known to be affected:

- Industrial DIN-Rail Device Server IDS-5042, all versions, and
- Industrial DIN-Rail Device Server IDS-5042+, all versions.

Note: Other ORing Industrial Networking products may also be affected by this vulnerability.

IMPACT

Attackers can exploit the product by using the default hard-coded credential to log into the device with administrative privileges. Once access is gained, the attacker can read and write to files and change settings. This access level can impact the availability, integrity and confidentiality of the product.

a. Korenix and ORing Use Crypto, http://www.digitalbond.com/2012/06/13/korenix-and-oring-insecurity/, Web site last accessed September 19, 2012.

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy/

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

BACKGROUND

ORing Industrial Networking is based in Taiwan and maintains offices in several countries around the world, including the US, Korea, and China.

The affected products are industrial serial device servers used for SCADA systems. According to ORing's Web site[b] are deployed across several sectors including manufacturing, oil and gas, transportation, electric utilities, and others. ICS-CERT estimates that these products are used primarily in the United States, Europe, and Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

USE OF HARD-CODED CREDENTIALS[c]

An attacker can log into the operating system of the device using an SSH connection with the root credentials to gain administrative access. Once the attacker gains access to the device, the file system and settings can be accessed, which could result in a loss of availability, integrity and confidentiality.

CVE-2012-4577[d] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[e]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

b. ORing Industrial Networking Corp., http://www.oring-networking.com/, Web site last visited September 19, 2012.

c. CWE, http://cwe.mitre.org/data/definitions/259.html, CWE-259: Use of Hard-coded Password, Web site last accessed September 18, 2012.

d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4577, Web site last visited September 19, 2012.

e. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C), Web site last visited September 19, 2012.

EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

ICS-CERT is not aware of ORing Industrial Networking developing a patch, update, or fix for the affected products. The ORing software update Web site[f] does not indicate that a new version of firmware or security patch is available.

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.[g] 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-12-146-01A—Cyber Intrusion Mitigation Strategies,[h] 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.

f. ORing Industrial DIN-Rail Device Server Update, http://www.oring-networking.com/support/product/sn/19, Web site last visited September 19, 2012.

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 19, 2012.

h. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 19, 2012.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks.

1. Do not click Web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams[i] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[j] for more information on social engineering attacks.

ICS-CERT CONTACT

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

Email: ics-cert@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.

i. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed September 19, 2012.

j. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed September 19, 2012.