



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-297-02—KORENIX JETPORT 5600 SERIES HARD-CODED CREDENTIALS

October 23, 2012

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts the Korenix JetPort 5600.

Independent researcher Reid Wightman of Digital Bond identified undocumented hard-coded root credentials^a in the firmware of the Korenix JetPort 5600 system application without coordination with ICS-CERT, the vendor, or any other coordinating entity known to ICS-CERT. The Korenix JetPort is an industrial serial device server to control multiple serial devices over Ethernet. Successful exploitation of this vulnerability would allow attackers to exploit the product by using the hard-coded credential to log into the device with administrative privileges and gain access to the attached serial devices. Korenix has produced an upgraded firmware version that removes the accounts. This product is used worldwide, primarily in the communications and information technology sectors.

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

AFFECTED PRODUCTS

The following Korenix products are affected:

- JetPort 5600, all versions.

IMPACT

Once access is gained, the attacker can read and write to the file system and reconfigure the device. Attackers may also have access to other serial devices that are attached to this product.

a. Korenix and ORing Use Crypto, <http://www.digitalbond.com/2012/06/13/korenix-and-oring-insecurity/>. Web site last accessed October 23, 2012.

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



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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

Korenix is a company based in Taiwan that was acquired by Beijer Electronics in 2010. Korenix maintains offices in several countries around the world, including the US, China, and Spain.

The JetPort 5600 series is a 4-port redundant serial device server that provides users with four serial interfaces. The device can control up to four serial devices over the Ethernet. Users can configure the device over HTTPS/SSH or by using the Korenix JetPort Commander software.

The affected products are industrial serial device servers used for SCADA systems. According to Korenix,^b they are deployed across several sectors including the communications (50%) and information technology (50%) sectors. Korenix estimates that these products are used worldwide, but the deployment depth is currently unknown.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

USE OF HARD-CODED CREDENTIALS^c

An attacker can log into the device using the hard-coded credentials that grant administrative access. Administrative credentials allow users to change device settings and read and write to the file system. This could result in a loss of confidentiality, integrity, or availability.

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

b. Korenix, <http://www.korenix.com>, Web site last accessed October 23, 2012.

c. CWE, <http://cwe.mitre.org/data/definitions/259.html>, CWE-259: Use of Hard-coded Password, Web site last accessed October 23, 2012.

d. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4577>, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

e. CVSS Calculator, [http://nvd.nist.gov/cvss.cfm?version=2&vector=\(AV:N/AC:L/Au:N/C:C/I:C/A:C\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)), Web site last accessed October 23, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely

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

Korenix has developed an upgraded version of firmware (v2.01) for the affected products. The upgraded firmware removes the root and guest accounts. The current version of OpenSSL (v0.9.8b) was also removed. The v2.01 firmware cannot be downgraded to v1.X.2 once upgraded. The Windows-based JetPort configuration tool, JetPort Commander, has also been upgraded to v3.0. The firmware upgrade can be downloaded from the Korenix software update Web site.^f

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 US-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.

f. Korenix JetPort Software Download, <http://www.korenix.com/jetport-5201-firmware.htm>, Web site last accessed October 23, 2012.

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 23, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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.

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.

h. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed October 23, 2012.

i. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed October 23, 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 October 23, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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.