IOActive Security Advisory

Title	ProSoft Technology RadioLinx ControlScape PRNG Vulnerability
Discovered by	Lucas Apa and Carlos Penagos
Advisory ID	ICSA-13-248-01
CVE	CVE-2013-2803
Disclosure	Coordinated with ICS-CERT
Severity	High
CVSS v2 Base Score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Impact Subscore	10
Exploitability Subscore	8.6

Background

ProSoft Technology is a US-based company with headquarters located in Bakersfield, California. Business offices are located worldwide in Europe, the Americas, and Asia. The affected product, ProSoft Technology RadioLinx ControlScape, is used for radio frequency communication with field-based automation controllers—primarily Rockwell Automation and Schneider Electric. The device provides connectivity between dissimilar systems over the Ethernet. ProSoft Technology wireless devices operate in high-interference environments by combining advanced frequency hopping and digital signal processing technology with outstanding receiver sensitivity and different types of antennas. According to ProSoft Technology, RadioLinx ControlScape software is deployed worldwide across several sectors including oil and gas, water and wastewater, and electric utilities.

Vulnerability Overview

The RadioLinx ControlScape application is used to configure and install radios in a FHSS radio network and to monitor their performance. ProSoft Technology states that default values built into the software work well for initial installation and testing. The software generates a random passphrase and sets the encryption level to 128-bit AES when it creates a new radio network.

This product uses the standard C runtime libraries calls `srand` and `rand` to seed and generate passphrases. Because it uses the local time as seed, an attacker could predict the default values built into the software. This makes the system vulnerable to expedited brute-force passphrase/password attacks and other cryptographic based attacks. Custom passphrases are not vulnerable to this type of attack. An attacker could compromise the device network and affect its data integrity, confidentiality, and availability.

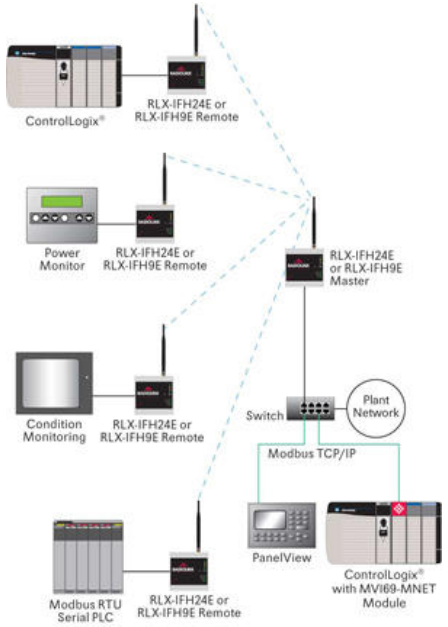
For more information please refer to the following White Paper:

http://www.ioactive.com/pdfs/Compromising_Industrial_Facilities_From_40_Miles-Away-Lucas_Apa_and_Carlos_Penagos.pdf

Affected Products

The following devices are affected by this vulnerability:

- RLX-FHE
- RLX-FHS
- RLX-FHES
- RLX-IFH24E-E
- RLX-IFH24S-E
- RLX-IFH24E-A
- RLX-IFH24S-A
- RLX-IFH9E-A
- RLX-IFH9S-A
- RLX-IFHE
- RLX-IFHS



Remediation

ProSoft Technology has released a new firmware patch, v6.00.040, which is available from the ProSoft Technology download page. IOActive did not verify the mentioned firmware patch:

http://www.prosoft-technology.com/SERVICES-SUPPORT/Downloads

Click on the ProSoft Software tab, then click on the ControlScape tab, and then click on the ControlScape FH v6.00.040 link to download the new firmware patch.

ProSoft has the following additional recommendations:

- Changing the default 'seed' passphrase will greatly increase the entropy of passphrase generation process.
- 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. 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 Mitigation Strategies, that is available for download from the ICS-CERT Web page (http://ics-cert.us-cert.gov/).

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.

