IOActive Uncover Vulnerability in Wireless Industrial Automation Software from ProSoft Technology

IOActive today announced that it has discovered a vulnerability in ProSoft Technology’s RadioLinx ControlScape application. The software is primarily used with Rockwell Automation and Schneider Electric solutions, and is deployed worldwide across several industries including oil and gas, water and wastewater, and electric utilities.

Seattle, Washington (PRWEB) October 23, 2013 -- IOActive, Inc., the leading global provider of specialist information security services, today announced that it has discovered a vulnerability in ProSoft Technology’s RadioLinx ControlScape application. The software is primarily used with Rockwell Automation and Schneider Electric solutions, and is deployed worldwide across several industries including oil and gas, water and wastewater, and electric utilities.

World authorities on Industrial Control Systems (ICS), Lucas Apa and Carlos Penagos, discovered the vulnerability in the industrial automation software. The software is used to configure and install radios in a Frequency Hoping (FH) network, as well as monitor the performance of the devices.

The software from ProSoft Technology generates a random passphrase and sets encryption levels to 128-bit Advanced Encryption Standard (AES) when it creates a new radio network. As the software uses the local time as the seed to generate passphrases, 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.

“Wireless radios used in Industrial Control Systems use software, like that from ProSoft Technology, to create and manage a new network. When a new network is created the software calculates a passphrase using a pseudorandom number generator,” said Lucas Apa, security researcher for IOActive. “The problem is that it uses the local time as the seed. This makes this algorithm predictable and weak, and vulnerable to expedited brute-force passphrase and other cryptographic-based attacks.”

Carlos Penagos, security researcher for IOActive added, “By being able to guess the passphrase, an attacker could communicate with the network the device is connected to with devastating consequences. For example, if an attacker is able to communicate with devices on the wireless network of a nuclear power plant, he could manipulate the data sent from these devices to industrial processes and cause dangerous consequences by overheating liquids or over pressurising chemicals, which in turn would result in catastrophic failure.”

On September 5, 2013, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published an advisory providing details of the vulnerability. ProSoft Technology has produced a new firmware patch to mitigate this vulnerability.

IOActive has also issued its own IOActive Labs Advisory outlining the affected products, the impact and the solution.

About IOActive
IOActive is a comprehensive, high-end information security services firm with a long and established pedigree in delivering elite security services to its customers. Our world-renowned consulting and research teams deliver
a portfolio of specialist security services ranging from penetration testing and application code assessment through to semiconductor reverse engineering. Global 500 companies across every industry continue to trust IOActive with their most critical and sensitive security issues. Founded in 1998, IOActive is headquartered in Seattle, USA, with global operations through the Americas, EMEA and Asia Pac regions. Visit www.ioactive.com for more information.
Contact Information
Craig Brophy
IOActive
http://www.ioactive.com
+44 7795662888

Online Web 2.0 Version
You can read the online version of this press release here.