ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-10-313-01— REALWIN BUFFER OVERFLOW

November 9, 2010

OVERVIEW

On October 15, 2010 an independent security researcher posted information[1] regarding vulnerabilities in RealFlex Technologies Ltd. RealWin SCADA software products. The security researcher's analysis indicated that successful exploitation of these vulnerabilities can lead to arbitrary code execution and control of the system.

RealFlex has validated the researcher's findings and released an update[2] to resolve these issues. ICS-CERT has verified that the software update resolves the vulnerabilities highlighted by the researcher.

AFFECTED PRODUCTS

All RealWin versions up to and including Version 2.1.8 (Build 6.1.8) are affected by these vulnerabilities.

IMPACT

RealWin is used in small installations for a variety of applications including monitoring water pumping stations, reservoirs, and water treatment plants.

Exploitation of these vulnerabilities may result in remote code execution. 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 environment, architecture, and product implementation.

BACKGROUND

RealFlex was established in 1982 and has offices in Limerick, Ireland; Houston, Texas; and Saratov, Russia. RealFlex products are used in more than 45 countries with primary sectors being power, oil and gas, water and wastewater, marine, transport, chemical, manufacturing, and telecommunications.

RealWin runs on Microsoft Windows platforms (2000 and XP). It can run on a single system or on multiple PCs connected through a TCP/IP network.

[1] Researcher, http://aluigi.altervista.org/adv/realwin_1-adv.txt, website last visited November 4, 2010.

[2] RealFlex, http://cs realflex.com/cs/index.ssp, website last visited November 8, 2010.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

According to the researcher's report, the service listening on TCP Port 912 is vulnerable to multiple stack-based buffer overflows from specially crafted packets. The stack-based buffer overflows are caused by use of the "sprintf" and "strcpy" functions in the RealWin software.

EXPLOITABILITY

An attacker with an intermediate skill level could create code to exploit these vulnerabilities. Organizations should be aware that a Metasploit[3] module is available for these vulnerabilities and the researcher has also made his exploit code publicly available.

MITIGATION

RealFlex has addressed these vulnerabilities with a software update available on the company's web site.[4]

The following mitigations are recommended:

- Update RealWin to Version 2.1.10 (Build 6.1.10).
- Ensure that your firewall is restricting access to TCP port 912. RealWin does not require external access to port 912 as it is only used internally on the PC between the communication modules and the RealWin module.
- Encourage asset owners to minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Control system networks and remote devices should be located behind firewalls, and be separate from the business network. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be utilized.
- Refer to the Control System Security Program Recommended Practices section for control systems on the US-CERT web site. Several recommended practices are available for reading or downloading, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[5]

As with all system changes, administrators should consult their control systems vendor prior to making any control system changes.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

RealWin customers who have any questions can contact RealFlex at security@realflex.com.

[3] Metasploit, http://www.metasploit.com, website last visited November 8, 2010.

4. RealFlex, http://cs realflex.com/cs/index.ssp, web site last visited November 8, 2010.

5. CSSP, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html, web site last visited November 8, 2010.

ICS-CERT CONTACT

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

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585

For Control System Security Program Information and Incident Reporting:
www.ics-cert.org

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.