ICS-CERT ADVISORY

ICSA-11-110-01—REALFLEX REALWIN MULTIPLE VULNERABILITIES

April 20, 2011

OVERVIEW

This ICS-CERT Advisory is a follow-up to the ICS-CERT Alert titled, "ICS-ALERT-11-080-04—Multiple Vulnerabilities in RealFlex RealWin."

An independent researcher has published exploit code for seven vulnerabilities identified in RealFlex Technologies' RealWin 2.1.10 Demo Supervisory Control and Data Acquisition (SCADA) product. Multiple functions listening on Port 910/TCP are susceptible to heap and stacked-based buffer overflow vulnerabilities. The heap and stack buffer overflows may allow an attacker to remotely execute arbitrary code.

RealFlex has released a new version (Version 2.1.12) of their free demo software that mitigates these vulnerabilities.

ICS-CERT has verified that these vulnerabilities do not affect the RealFlex RealWin commercial version and that Version 2.1.12 resolves the vulnerabilities in the demo version.

AFFECTED PRODUCTS

RealFlex reports that these zero-day vulnerabilities affect Versions 1.06A and earlier of its demo software only. The commercial version of RealWin is not affected.

IMPACT

Successful exploitation of these vulnerabilities can cause the RealWin demo application to crash.

BACKGROUND

RealFlex Technologies Ltd is a company based in Houston, Texas, that focuses on industrial automation software for many markets including power, oil and gas, water and wastewater, chemical, transportation, and manufacturing. RealWin is a SCADA server product including a human-machine interface that runs on a Windows (XP or newer) platform. For more information on RealFlex and RealWin, visit their website at: www.realflex.com.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The researcher provided reports of seven separate vulnerabilities. Six are stack overflows that can be exploited remotely. The remaining vulnerability is an integer overflow that also can be exploited remotely.

Multiple functions listening on Port 910/TCP are susceptible to these buffer overflow vulnerabilities.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from a remote machine.

EXISTENCE OF EXPLOIT

The researcher has publicly released exploits that specifically target these vulnerabilities.

DIFFICULTY

An attacker would need only basic skills to use the publicly available code to exploit these vulnerabilities.

MITIGATION

Users of the demo version of RealFlex RealWin should upgrade to the newest version (2.1.12) which is available at http://realflex.com/download/.

ICS-CERT encourages 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 isolated from the business network. If remote access is required, use secure methods such as Virtual Private Networks (VPNs).

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

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[a]

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.

a. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, accessed March 3, 2011.