ICS-CERT ALERT

ICS–ALERT-11-080-04—MULTIPLE VULNERABILITIES IN REALFLEX REALWIN

March 21, 2011

ALERT

SUMMARY

An independent researcher has published eight vulnerabilities with exploit code in RealFlex Technologies' RealWin Supervisory Control and Data Acquisition (SCADA) product. Multiple functions listening on 910/TCP and 912/TCP are susceptible to heap and stacked-based buffer overflow vulnerabilities. The heap and stack buffer overflows may allow remote execution of arbitrary code.

ICS-CERT is currently coordinating with the vendor and security researcher to identify additional mitigations. ICS-CERT will provide additional information as it becomes available.

MITIGATION

ICS-CERT recommends that users minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[1] Locate control system networks and devices behind firewalls, and isolate them from the business network. If remote access is required, employ 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.*[2]

1. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed January 17, 2011.

2. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

BACKGROUND

RealWin is a SCADA server that includes a human-machine interface (HMI) application. It 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.

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.

ICS-CERT CONTACT

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

ICS-CERT Operations Center
1-877-776-7585

www.ics-cert.org
ICS-CERT@DHS.GOV

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.