ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-10-305-01 - REALWIN BUFFER OVERFLOW VULNERABILITIES

November 1, 2010

ALERT

SUMMARY

An independent security researcher has published information regarding vulnerabilities in RealFlex's Realwin SCADA software product to a vulnerability disclosure web site. ICS-CERT has reached out to both RealFlex and the security researcher and will continue to work with the vendor to validate the researcher's claim.

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.

RealWin is a SCADA server product, which includes an HMI and runs on Windows 2000 and XP. 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 is coordinating this vulnerability with the CERT Coordination Center.

RECOMMENDED MITIGATIONS

ICS-CERT recommends:

- Placing all control systems assets behind firewalls, separated from the business network.
- Implementing network or host-based firewall rules to limit network access to TCP port 912.
- Deploying secure remote access methods such as Virtual Private Networks (VPNs) for remote access.

ICS-CERT will provide additional information as it becomes available.

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.