ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-245-01— MULTIPLE ACTIVEX VULNERABILITIES IN ADVANTECH BROADWIN WEBACCESS

September 02, 2011

ALERT

SUMMARY

ICS-CERT has become aware of two publicly disclosed vulnerabilities with and proof of concept code affecting the Advantech BroadWin WebAccess Client 1.0.0.10, a web browser-based human-machine interface (HMI) product. The public disclosure indicates that these vulnerabilities are remotely exploitable. ICS-CERT has contacted and is coordinating this information with Advantech to validate and confirm this report.

Specifically, the two disclosed vulnerabilities are:

- A format string vulnerability
- A memory corruption vulnerability

ICS-CERT will provide additional information as it becomes available. Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

BACKGROUND

Advantech BroadWin WebAccess is a web-based HMI platform used in energy, manufacturing, and building automation applications. WebAccess is installed in several countries in Asia, North America, North Africa, and the Middle East.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ICS-CERT@DHS.GOV

For Control Systems Security Program (CSSP) Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

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.