



ICS-CERT ALERT

ICS-ALERT-11-306-01—ADVANTECH BROADWIN WEBACCESS ACTIVEX VULNERABILITY

November 2, 2011

ALERT

SUMMARY

ICS-CERT is aware of a public report detailing an ActiveX vulnerability with proof-of-concept (PoC) exploit code affecting Advantech Broadwin WebAccess. This is a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, the vulnerability is exploitable by targeting the bwocxrun.ocx ActiveX component with a combination of ActiveX methods. This report was released without coordination with either the vendor or the ICS-CERT.

ICS-CERT has not yet verified this vulnerability or PoC code but has reached out to the affected vendor to notify, confirm, and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The report included vulnerability details and PoC exploit code for the following vulnerability:

Vulnerability Type	Exploitability	Impact
Buffer Overflow	Remote	Possible Remote Code Execution

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.

MITIGATION

ICS-CERT is currently coordinating with the vendor to identify mitigations.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.^a
- 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), recognizing that VPN is only as secure as the connected devices.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*^b for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*^c for more information on social engineering attacks.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) 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*.^d

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 CONTACT

ICS-CERT Operations Center

1-877-776-7585

ICS-CERT@DHS.GOV

For CSSP Information and Incident Reporting: www.ics-cert.org

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed November 02, 2011.

b. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed November 02, 2011

c. National Cyber Alert System Cyber Security Tip ST04-014, <http://www.us-cert.gov/cas/tips/ST04-014.html>, website last accessed November 02, 2011

d. Control Systems Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 02, 2011.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is provided when prior coordination has occurred either with the vendor, ICS-CERT, or other coordinating entity. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.