ICS-CERT ALERT

ICS-ALERT-13-009-01—ADVANTECH WEBACCESS CROSS SITE SCRIPTING VULNERABILITY

January 9, 2013

ALERT

SUMMARY

ICS-CERT is aware of a public report of a cross-site scripting vulnerability with proof-of-concept (PoC) exploit code affecting the Advantech WebAccess, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to the report, this cross-site scripting vulnerability could allow a remote authenticated attacker to execute arbitrary code in a user's browser session.

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.

This report was released by Antu Sanadi of SecPod Technologies without successful coordination of the vendor.

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

Vulnerability Type	Remotely Exploitable	Impact
Cross-site Scripting	Yes	Execute unauthorized code; bypass protection mechanisms; read application data

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

MITIGATION

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

- 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.

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

ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[b]

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
Email: ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting: www.ics-cert.org.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed January 09, 2013.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 09, 2013.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. 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.