ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ALERT

ICS-ALERT-12-039-01—ADVANTECH BROADWIN RPC SERVER VULNERABILITY

February 08, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report about an RPC server vulnerability with proof-of-concept (PoC) exploit code affecting the Advantech BroadWin WebAccess software, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, the WebAccess software is vulnerable to an RPC exploit against the WebAccess network service on either Port 4592/TCP or 14592/TCP. This report was released by amisto0x07 and Z0mb1E without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified the affected vendor of this report. ICS-CERT has also determined, that while similar to the report by Rubén Santamarta identified in "ICS-ALERT-11-081-01 – BroadWin WebAccess", this exploit targets a different vulnerability in the RPC service.

ICS-CERT is issuing this alert to provide early notice of this report and to identify baseline mitigations for reducing risks to this and other cybersecurity attacks.

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

Vulnerability Type	Exploitability	Impact
Missing Authentication for Critical Function[a]	Remote	Possible Remote Code Execution / Denial of Service

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

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:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[b]

[a] http://cwe.mitre.org/data/definitions/306.html, website last accessed February 08, 2012

[b] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed February 08, 2012.

- Locate control system networks and devices behind properly configured firewalls addressing access to Port 4592/TCP or 14592/TCP, 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.

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.*[c]

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

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 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.

[c] Control Systems Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed February 08, 2012.