ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-094-02A—ADVANTECH/BROADWIN WEBACCESS RPC VULNERABILITY

UPDATE A

November 04, 2011

OVERVIEW

This Advisory Update is a follow-up to the original Advisory titled “ICSA-11-094-02 – Advantech/BroadWin WebAccess RPC Vulnerability”[a] that was published April 4, 2011, on the ICS-CERT web page. That Advisory was preceded by Alert “ICS-ALERT-11-081-01 – BroadWin WebAccess”[b] that was published March 22, 2011.

Independent security researcher Rubén Santamarta has identified details and released exploit code for a Remote Procedure Call (RPC) vulnerability in Advantech/BroadWin WebAccess. This is a web browser-based human-machine interface (HMI) product. This RPC vulnerability affects the WebAccess Network Service on 4592/TCP and allows remote code execution.

--------- Begin Update A Part 1 of 3 --------

Advantech/BroadWin has notified ICS-CERT that a patch will not be issued to address this vulnerability.

--------- End Update A Part 1 of 3 ----------

AFFECTED PRODUCTS

This vulnerability affects all versions of Advantech/BroadWin WebAccess.

IMPACT

The successful exploit of this vulnerability could allow an attacker to remotely execute arbitrary code.

The full impact to individual organizations is dependent on multiple factors unique to each organization. The ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and operational product implementation.

BACKGROUND

Advantech/BroadWin WebAccess is a web-based HMI product used in energy, manufacturing, and building automation systems. The installation base is across Asia, North America, North Africa, and the Middle East. WebAccess Client is available for desktop computers and laptops running Windows 2000,

[a] http://www.us-cert.gov/control_systems/pdf/ICSA-11-094-02.pdf, website last accessed November 04, 2011.

[b] http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-081-01.pdf, website last accessed November 04, 2011.

XP, Vista, and Server 2003. A thin-client interface is available for Windows CE and Windows Mobile 5.0.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

This vulnerability exploits an RPC vulnerability in Advantech/Broadwin WebAccess Network Service on 4592/TCP.

--------- Begin Update A Part 2 of 3 --------

CVE-2011-4041[c] has been assigned to this vulnerability in the National Vulnerability Database.

--------- End Update A Part 2 of 3 ----------

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker can initiate this exploit from a remote machine without user interaction.

EXISTENCE OF EXPLOIT

An exploit of this vulnerability has been posted publicly.

DIFFICULTY

This vulnerability requires a moderate level of skill to exploit.

MITIGATION

--------- Begin Update A Part 3 of 3 --------

Advantech Broadwin has no plans to issue a patch to address this vulnerability.

--------- End Update A Part 3 of 3 ----------

Prior to the release of the patch, customers using Advantech/BroadWin WebAccess should refer to security considerations recommended by BroadWin in their Installation Manual.[d]

For further assistance, contact BroadWin support at support@broadwin.com.

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.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4041

[d] WebAccess Installation Guide, BroadWin, http://broadwin.com/Manual/InstallGuide/InstallGuide.htm, accessed March 31, 2011.

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

The Control Systems Security Program 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.*[e]

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For Control Systems Security Program Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

[e] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, accessed March 31, 2011.