Advantech/Broadwin WebAccess RPC Vulnerability (Update B) | CISA

Published: 2018-09-06 · Archived: 2026-04-05 21:52:03 UTC

OVERVIEW

This updated advisory is a follow-up to the updated advisory titled ICSA-11-094-02A Advantech/Broadwin WebAccess RPC Vulnerability that was published November 4, 2011, on the NCCIC/ICS-CERT Web site.

--------- Begin Update B Part 1 of 5 --------

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

Advantech has provided a free version upgrade that mitigates this vulnerability for any licensed user of any previous version of WebAccess.

--------- End Update B Part 1 of 5 ----------

AFFECTED PRODUCTS

--------- Begin Update B Part 2 of 5 --------

This vulnerability affects all versions of WebAccess prior to Version 7.1 2013.05.30, including all legacy versions of either Advantech WebAccess or BroadWin WebAccess.

--------- End Update B Part 2 of 5 ----------

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 NCCIC/ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and operational product implementation.

BACKGROUND

--------- Begin Update B Part 3 of 5 --------

Advantech/Broadwin WebAccess is a Web-based HMI product used in energy, manufacturing, and building automation systems. The installation base is across Asia; North, Central, and South America; North Africa; the Middle East; and Europe. WebAccess Client software is available for desktop computers and laptops running Windows 2000, XP, Vista, Server 2003, Windows 7, and Windows 8. A thin-client interface is available for Windows CE and Windows Mobile 5.0.

--------- End Update B Part 3 of 5 ----------

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

--------- Begin Update B Part 4 of 5 --------

CODE INJECTIONCWE-94: Improper Control of Generation of Code ('Code Injection'), http://cwe.mitre.org/data/definitions/94.html, Web site last accessed January 07, 2014.

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

CVE-2011-4041NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4041, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory. has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C, Web site last accessed January 07, 2014.

--------- End Update B Part 4 of 5 ----------

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 B Part 5 of 5 --------

Advantech has released a new version of WebAccess that mitigates this vulnerability. Users may upgrade to the latest version from any previous version of WebAccess at no charge. Download the latest version of WebAccess (V 7.1 2013.05.30) from the following location on the Advantech Web site:

http://support.advantech.com.tw/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download.

Advantech has also created the following site to share additional information about WebAccess:

http://webaccess.advantech.com/ .

Prior to the release of this new version, customers using WebAccess should refer to security considerations recommended by Advantech in the WebAccess Installation Manual:

http://advantech.vo.llnwd.net/o35/www/webaccess/driver_manual/Advantech-WebAccess-User-Manual.chm.

For further assistance, contact Advantech support at +1-877-451-6868.

--------- End Update B Part 5 of 5 ----------

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to NCCIC/ICS-CERT for tracking and correlation against other incidents.
NCCIC/ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

NCCIC/ICS-CERT also provides a section for control systems security recommended practices on the NCCIC/ICS-CERT Web site at: http://ics-cert.us-cert.gov/content/recommended-practices. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.
