ICSA-14-079-03

Information source https://ics-cert.us-cert.gov/advisories/ICSA-14-079-03

Advantech has created a new version (Version 7.2) that mitigates each of the vulnerabilities described above. Users may download this version from the following location at their web site webaccess.advantech.com.

OVERVIEW

This advisory is a follow-up to the original advisory titled "ICSA-14-079-03P Advantech WebAccess Vulnerabilities" that was posted to the US-CERT secure Portal library March 20, 2014.

Researchers working with HP's Zero Day Initiative (ZDI), Andrea Micalizzi, aka rgod, Tom Gallagher, and an independent anonymous researcher, have identified several vulnerabilities in Advantech's WebAccess application. ZDI reported them to NCCIC/ICS-CERT. Advantech has produced a new version that mitigates these vulnerabilities.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following Advantech WebAccess versions are affected:

WebAccess Version 7.1 and previous.

IMPACT

An attacker may be able to exploit these vulnerabilities to execute arbitrary code and view contents of files stored on the target machine.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Advantech is based in Taiwan and has distribution offices in 21 countries worldwide.

Advantech WebAccess, formerly known as BroadWin WebAccess, is a web-based SCADA and human-machine interface product used in energy, critical manufacturing, commercial facilities, and government facilities. These systems are deployed globally.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

SQL INJECTION

An attacker using SQL injection may use arguments to construct queries without proper sanitization. The DBVisitor.dll is exposed through SOAP interfaces, and the exposed functions are vulnerable to SOAP injection. This may allow unexpected SQL action and access to records in the table of the software database or execution of arbitrary code.

CVE-2014-0763 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).c

STACK BUFFER OVERFLOW

By providing an overly long string to the NodeName parameter, an attacker may be able to overflow the static stack buffer. The attacker may then execute code on the target device remotely.

CVE-2014-0764 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).f

STACK BUFFER OVERFLOW

To exploit this vulnerability, the attacker sends data from the GotoCmd argument to control. If the value of the argument is overly long, the static stack buffer can be overflowed. This will allow the attacker to execute arbitrary code remotely.

CVE-2014-0765 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).i

STACK BUFFER OVERFLOW

An attacker can exploit this vulnerability by copying an overly long NodeName2 argument into a statically sized buffer on the stack to overflow the static stack buffer. An attacker may use this vulnerability to remotely execute arbitrary code.

CVE-2014-0766 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).l

STACK BUFFER OVERFLOW

An attacker may exploit this vulnerability by passing an overly long value from the AccessCode argument to the control. This will overflow the static stack buffer. The attacker may then execute code on the target device remotely.

CVE-2014-0767 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).

STACK BUFFER OVERFLOW

An attacker may pass an overly long value from the AccessCode2 argument to the control to overflow the static stack buffer. The attacker may then remotely execute arbitrary code.

CVE-2014-0768 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).r

STACK BUFFER OVERFLOW

By providing an overly long string to the UserName parameter, an attacker may be able to overflow the static stack buffer. The attacker may then execute code on the target device remotely.

CVE-2014-0770 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).

INFORMATION DISCLOSURE

The BWOCXRUN.BwocxrunCtrl.1 control contains a method named "OpenUrlToBuffer." This method takes a URL as a parameter and returns its contents to the caller in JavaScript. The URLs are accessed in the security context of the current browser session. The control does not perform any URL validation and allows "file://" URLs that access the local disk.

The method can be used to open a URL (including file URLs) and read file URLs through JavaScript. This method could also be used to reach any arbitrary URL to which the browser has access.

CVE-2014-0771 has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).

INFORMATION DISCLOSURE

The BWOCXRUN.BwocxrunCtrl.1 control contains a method named OpenUrlToBufferTimeout. This method takes a URL as a parameter and returns its contents to the caller in JavaScript. The URLs are accessed in the security context of the current browser session. The control does not perform any URL validation and allows file:// URLs that access the local disk.

The method can be used to open a URL (including file URLs) and read the URLs through JavaScript. This method could also be used to reach any arbitrary URL to which the browser has access.

CVE-2014-0772 has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).

COMMAND INJECTION

The BWOCXRUN.BwocxrunCtrl.1 control contains a method named "CreateProcess." This method contains validation to ensure an attacker cannot run arbitrary command lines. After validation, the values supplied in the HTML are passed to the Windows CreateProcessA API.

The validation can be bypassed allowing for running arbitrary command lines. The command line can specify running remote files (example: UNC command line).

A function exists at offset 100019B0 of bwocxrun.ocx. Inside this function, there are 3 calls to strstr to check the contents of the user specified command line. If "\setup.exe," "\bwvbprt.exe," or "\bwvbprtl.exe" are contained in the command line

(strstr returns nonzero value), the command line passes validation and is then passed to CreateProcessA.

CVE-2014-0773 has been assigned to this vulnerability. A CVSS v2 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:P).

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with low skill would be able to exploit these vulnerabilities.

MITIGATION

Advantech has created a new version (Version 7.2) that mitigates each of the vulnerabilities described above. Users may download this version from the following location at their web site:

http://webaccess.advantech.com/downloads.php?item=software

For additional information about WebAccess, please visit the following Advantech web site:http://webaccess.advantech.com/

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at http://ics-cert.us-cert.gov/content/recommended-practices. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B-Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.