ICSA-14-198-02

Information source https://ics-cert.us-cert.gov/advisories/ICSA-14-198-02

Advantech released a new WebAccess Installation Package v7.2 on June 6, 2014, that removes some vulnerable ActiveX components and resolves the vulnerabilities within others. The download link for v7.2 is available at webaccess.advantech.com.

OVERVIEW

NCCIC/ICS-CERT received a report from the Zero Day Initiative (ZDI) concerning vulnerabilities affecting the Advantech WebAccess application. These vulnerabilities were reported to ZDI by security researchers Dave Weinstein, Tom Gallagher, John Leitch, and others. Advantech has produced an updated software version that mitigates these vulnerabilities.

These vulnerabilities could be exploited remotely. Exploits that target these vulnerabilities are known to be publicly available.

AFFECTED PRODUCTS

The following Advantech WebAcess versions are affected:

- Advantech WebAcess v7.1 and earlier.

IMPACT

An attacker exploiting these vulnerabilities in WebAccess may be able to bypass authentication or cause a denial of service.

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

STACK-BASED BUFFER OVERFLOWS

There are multiple ways to overflow the static stack buffer by providing overly long strings to specific parameters (namely ProjectName, SetParameter, NodeName, CCDParameter, SetColor, AlarmImage, GetParameter, GetColor, ServerResponse, SetBaud, and IPAddress) within the webvact.ocx, dvs.ocx, and webdact.ocx ActiveX files.

CVE-2014-2364 has been assigned to these vulnerabilities. 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).

UNSAFE ACTIVEX CONTROL MARKED SAFE FOR SCRIPTING

The bwocxrun ActiveX control (installed by default as part of setup) allows navigation from the Internet to a local file. This is accomplished through the BrowseFolder method.

CVE-2014-2368 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).

REMOTE AUTHENTICATION BYPASS

The ChkCookie subroutine within broadweb\include\gChkCook.asp ActiveX control (installed by default as part of setup) allows navigation from the Internet to a local file. If user, proj, and scada are set, and bwuser is set to true, this will grant access to several previously restricted pages.

CVE-2014-2367 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

PASSWORD DISCLOSURE

The upAdminPg.asp component includes the password of the specified account in the underlying HTML when serving the page.

CVE-2014-2366 has been assigned to this vulnerability. A CVSS v2 base score of 9.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:C/I:C/A:C).

REMOTE CODE EXECUTION

Advantech WebAccess contains a flaw that enables a malicious user to arbitrarily create and delete files.

CVE-2014-2365 has been assigned to this vulnerability. A CVSS v2 base score of 6.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:S/C:P/I:P/A:P).

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target these vulnerabilities are publicly available.

DIFFICULTY

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

MITIGATION

Advantech released a new WebAccess Installation Package v7.2 on June 6, 2014, that removes some vulnerable ActiveX components and resolves the vulnerabilities within others. The download link for v7.2 is available at:

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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize 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 (http://ics-cert.us-cert.gov/).

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