ICS-CERT ADVISORY

ICSA-12-047-01—ADVANTECH WEBACCESS MULTIPLE VULNERABILITIES

February 16, 2012

OVERVIEW

This advisory follows up on two previous ICS-CERT Alerts:

- "ICS-ALERT-11-245-01—Multiple ActiveX Vulnerabilities in Advantech BroadWin WebAccess," published September 2, 2011[a]
- "ICS-ALERT-11-306-01—Advantech BroadWin WebAccess ActiveX Vulnerability," published November 2, 2011.[b]

ICS-CERT received both coordinated and uncoordinated reports of eighteen vulnerabilities in BroadWin WebAccess. These vulnerabilities include:

- Cross-site scripting (XSS)
- SQL injection
- Cross-site report forgery (CSRF)
- Authentication issues.

These vulnerabilities were reported separately by the nSense Vulnerability Coordination Team, Greg MacManus of iSIGHT Partners, Kuang-Chun Hung of Security Research and Service Institute–Information and Communication Security Technology Center (ICST), Luigi Auriemma, and Snake (alias).

ICS-CERT has coordinated with Advantech, which has released a new version of WebAccess that addresses most of the reported vulnerabilities.

AFFECTED PRODUCTS

These vulnerabilities affect all versions of Advantech/BroadWin WebAccess prior to applying the patch (V7.0) listed in the mitigations below.

a. http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-245-01.pdf, ICS-ALERT-11-245-01, website last accessed February 15, 2012.
b. http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-306-01.pdf, ICS-ALERT-11-306-01, website last accessed February 15, 2012.

IMPACT

An attacker can bypass authentication, gain administrative privileges, and remotely execute arbitrary code by exploiting these vulnerabilities.

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

BACKGROUND

Advantech/BroadWin WebAccess is a web-based human-machine interface 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 computers running Windows 2000, XP, Vista, and Server 2003. A thin-client interface is available for Windows CE and Windows Mobile 5.0.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

1. CROSS-SITE SCRIPTING[c]

An attacker may use a malformed URL address in a XSS attack to launch JavaScript code.

CVE-2012-0233[d] has been assigned to this vulnerability.

2. SQL INJECTION[e]

An attacker can use a malformed URL address to execute an SQL injection attack.

CVE-2012-0234[f] has been assigned to this vulnerability.

c. http://cwe.mitre.org/data/definitions/79.html, CWE-79: Cross Site Scripting, website last accessed February 15, 2012
d. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0233, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
e. http://cwe.mitre.org/data/definitions/89.html, CWE-89: SQL Injection, website last accessed February 15, 2012
f. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0234, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

3. CROSS-SITE REQUEST FORGERY[g]

The web application does not sufficiently verify whether a request was intentionally provided by the user who submitted the request.

CVE-2012-0235[h] has been assigned to this vulnerability.

4. INFORMATION LEAKAGE[i]

An unauthenticated user can access restricted information using specific URL addresses.

CVE-2012-0236[j] has been assigned to this vulnerability.

5. UNAUTHORIZED MODIFICATION

This vulnerability can be exploited by using specifically crafted URL addresses, which allows an unauthenticated user to enable or disable date and time syncing.

CVE-2012-0237[k] has been assigned to this vulnerability.

6. STACK-BASED BUFFER OVERFLOW[l]

A stack-based buffer overflow vulnerability exists in opcImg.asp that, when exploited, allows an attacker to remotely execute arbitrary code.

CVE-2012-0238[m] has been assigned to this vulnerability.

7. AUTHENTICATION VULNERABILITY[n]

An authentication vulnerability exists in uaddUpAdmin.asp in Advantech's WebAccess 7.0—and possibly earlier versions—that, when exploited, allows an attacker to remotely change an administrator's password. Exploit code is not required to exploit this vulnerability.

CVE-2012-0239[o] has been assigned to this vulnerability.

---

g. http://cwe.mitre.org/data/definitions/352.html, CWE-352: Cross-Site Request Forgery, website last accessed February 15, 2012
h. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0235, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
i. http://cwe.mitre.org/data/definitions/200.html, CWE-200: Information Exposure, website last accessed February 15, 2012
j. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0236, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
k. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0237, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
l. http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, website last accessed February 15, 2012
m. http://web.nvd.nist.gov/view/vuln/detail?vulnId= CVE-2012-0238, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
n. http://cwe.mitre.org/data/definitions/287.html, CWE-287: Improper Authentication, website last accessed February 15, 2012

8. AUTHENTICATION VULNERABILITY[p]

An authentication vulnerability exists in GbScriptAddUp.asp that, when exploited, allows an attacker to remotely execute arbitrary code.

CVE-2012-0240[q] has been assigned to this vulnerability.

9. ACTIVEX BUFFER OVERFLOW[r]

A long string input to ActiveX parameters will cause a buffer overflow, which might allow remote attackers to execute arbitrary code and gain full control of the server.

CVE-2011-4526[s] has been assigned to this vulnerability.

10. BUFFER OVERFLOW[t]

This vulnerability exists because long string input to parameters will cause a buffer overflow, which could allow execution of arbitrary code.

CVE-2011-4524[u] has been assigned to this vulnerability.

11. FILE MANIPULATION

An attacker can load any remote web page and write to a local batch file that will allow arbitrary code execution.

CVE-2011-4525[v] has been assigned to this vulnerability.

12. SQL INJECTION[w]

This vulnerability exists because string inputs are not checked, allowing attackers to perform SQL injection attacks.

---

o. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0239, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
p. http://cwe.mitre.org/data/definitions/287.html, CWE-287: Improper Authentication, website last accessed February 15, 2012.
q. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0240, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
r. http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, website last accessed February 15, 2012.
s. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4526, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
t. http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, website last accessed February 15, 2012.
u. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4524, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
v. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4525, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
w. http://cwe.mitre.org/data/definitions/89.html, CWE-89: SQL Injection, website last accessed February 15, 2012.

CVE-2011-4521[x] has been assigned to this vulnerability.

13. CROSS-SITE SCRIPTING[y]

This vulnerability exists because malicious cross-site scripts are allowed by parameters of bwerrdn.asp.

CVE-2011-4522[z] has been assigned to this vulnerability.

14. CROSS-SITE SCRIPTING[aa]

This vulnerability exists because malicious cross-site scripts are allowed by parameters of bwview.asp.

CVE-2011-4523[bb] has been assigned to this vulnerability.

15. ARBITRARY MEMORY CORRUPTION[cc]

This vulnerability exists because functions are allowed to corrupt arbitrary memory zones through fully controllable stream identifiers.

CVE-2012-0241[dd] has been assigned to this vulnerability.

16. FORMAT STRING[ee]

A format string vulnerability can be exploited by the using a message string without the required format arguments.

CVE-2012-0242[ff] has been assigned to this vulnerability.

x. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4521, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
y. http://cwe.mitre.org/data/definitions/79.html, CWE-79: Cross Site Scripting
z. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4522, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
aa. http://cwe.mitre.org/data/definitions/79.html, CWE-79: Cross Site Scripting, website last accessed February 15, 2012.
bb. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4523, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
cc. http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, website last accessed February 15, 2012.
dd. http://web.nvd.nist.gov/view/vuln/detail?vulnId= CVE-2012-0241, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
ee. http://cwe.mitre.org/data/definitions/134.html, CWE-134: Uncontrolled Format String, website last accessed February 15, 2012.
ff. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0242, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

17. ACTIVEX BUFFER OVERFLOW[gg]

A component used by WebAccess, bwocxrun.ocx, is vulnerable to a buffer overflow vulnerability due to methods that are capable of creating a arbitrary file in arbitrary location. Exploitation could allow the execution of arbitrary code.

CVE-2012-0243[hh] has been assigned to this vulnerability.

18. SQL INJECTION[ii]

This vulnerability exists because string inputs are not checked on input, allowing attackers to perform many different SQL injection attacks.

CVE-2012-0244[jj] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

All the vulnerabilities contained in this report are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with low to moderate skill can exploit these vulnerabilities.

MITIGATION

Advantech has created a new version of WebAccess (7.0) that addresses these vulnerabilities.[kk] This new version can be obtained at: http://webaccess.advantech.com/downloads.php. Advantech recommends that the new version be installed over the existing installation. If the existing version of WebAccess is uninstalled, the computer must be rebooted before reinstalling WebAccess.

gg. http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, website last accessed February 15, 2012.
hh. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0243, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
ii. http://cwe.mitre.org/data/definitions/89.html, CWE-89: SQL Injection, website last accessed February 15, 2012.
jj. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0244, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
kk. Advantech WebAccess security update, http://webaccess.advantech.com/security.php, website last accessed February 15, 2012.

Advantech recommends that customers using the WebAccess product refer to security considerations recommended by their installation manual.[ll]

For further assistance, customers should contact BroadWin support at support@broadwin.com.[mm]

ICST, iSIGHT, and ICS-CERT have validated that the new version mitigates Vulnerabilities 1 and 5–16. For Vulnerabilities 2 and 3, the patched version fixes the issue for unauthenticated users; however, the problem still remains for nonadmin project users. Vulnerability 4 was not patched, because Advantech does not consider it to be a security risk. Neither ICS-CERT nor independent researchers have validated that the new version resolves Vulnerabilities 17 and 18.

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. Critical devices should not directly face 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.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[nn] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[oo] for more information on avoiding e-mail scams

ll. WebAccess Quick Installation Guide, BroadWin, http://broadwin.com/Manual/InstallGuide/InstallGuide.htm , website last accessed February 15, 2012.

mm. WebAccess customer notification, http://www.advantechdirect.com/eMarketingPrograms/WebAccess_Patch/WebAccess_Vulnerability.htm , website last accessed February 15, 2012.

nn. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed February 09, 2012.

oo. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed February 15, 2012

3. Refer to *Avoiding Social Engineering and Phishing Attacks*[pp] for more information on social engineering attacks.

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 CSSP 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.

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.

pp. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed February 15, 2012