ICS-CERT ADVISORY

ICSA-12-095-01—ABB MULTIPLE COMPONENTS BUFFER OVERFLOW

April 04, 2012

OVERVIEW

Independent researchers Terry McCorkle and Billy Rios identified a buffer overflow vulnerability in multiple components of the ABB WebWare Server application These components have been found to contain vulnerabilities in the COM and scripting interfaces. Follow-up investigation by ABB showed that these components are used in multiple ABB legacy products.

Because these are legacy products nearing the end of their life cycle, ABB does not intend to patch these vulnerable components.

AFFECTED PRODUCTS

The following ABB products are affected:

- WebWare Server: All versions of included Data Collector and Interlink
- WebWare SDK: All versions
- ABB Interlink Module: All versions
- S4 OPC Server: All versions
- QuickTeach: All versions
- RobotStudio S4: All versions
- RobotStudio Lite: All versions.

IMPACT

Successfully exploiting these vulnerabilities could lead to a denial-of-service for the application and privilege escalation or could allow an attacker to execute arbitrary code.

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

The legacy WebWare software products include a number of COM and ActiveX controls. These controls are delivered and installed together in the above products to facilitate communications with the robot controller or the WebWare Server and may run as services on the PC. Other controls provide graphical elements for web pages and custom human-machine interfaces (HMIs).

The above products are used in several different roles in a factory environment. WebWare Server is used for data gathering and backup handling. WebWare SDK, ABB Interlink Module, and S4 OPC Server are used for HMIs and communications to and from a robot controller. QuickTeach, RobotStudio S4, and RobotStudio Lite are PC tools used for training, installation, and programming of a robot cell.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

According to independent researchers Terry McCorkle and Billy Rios, multiple components of the ABB WebWare Server application contain a buffer overflow vulnerability. According to ABB, the legacy PC products WebWare Server, WebWare SDK, and other legacy products that include parts of WebWare contain a number of COM and ActiveX components that have been found to contain vulnerabilities in the COM and scripting interfaces. Follow-up investigation by ABB showed that these components are used in multiple ABB platforms.

VULNERABILITY DETAILS

STACK-BASED BUFFER OVERFLOW[a]

The COM and ActiveX controls included in the software do not provide adequate checking of input data. A user or program could call one of the controls' interfaces with specially crafted input data that can overflow the stack pointer or cause the control to stop execution. The ActiveX controls have been registered as scriptable, which means that they can be included and scripted from remotely served web pages.

CVE-2012-1801[b] has been assigned to this vulnerability. According to ABB, a CVSS Overall Score of 7.7 has also been assigned.

EXPLOITABILITY

The vulnerability in these components is remotely exploitable.

a. http://cwe.mitre.org/data/definitions/119.html, "CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer," website last accessed April 03, 2012.

b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1801, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

EXISTENCE OF EXPLOIT

No known exploits specifically target these vulnerable components.

DIFFICULTY

Crafting a working exploit for this vulnerability requires a medium skill level.

MITIGATION

According to ABB, the WebWare Server and the products listed above are legacy products nearing the end of their life cycle that are no longer actively supported. Users of these products are directed to the available documentation on mitigating risk and securing their machines and production environments. Because these are legacy products, ABB does not intend to patch these vulnerable components.

ABB customers using these products may contact their local ABB Robotics service organization (see www.abb.com for information).

Questions or responses on cybersecurity may be addressed to: cybersecurity@ch.abb.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. 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.*[c] 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.

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 03, 2012.

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.