ICS-CERT ADVISORY

ICSA-12-320-01—ABB AC500 PLC WEBSERVER BUFFER OVERFLOW VULNERABILITY

November 15, 2012

OVERVIEW

ICS-CERT has been notified of a buffer overflow vulnerability in the ABB AC500 PLC Webserver application. Successful exploitation of this vulnerability could lead to a denial of service (DoS), affecting the availability of the service. This vulnerability is related to ICS-CERT Advisory, ICSA-12-006-01—3S Smart Software Solutions CoDeSys Vulnerabilities[a] as the ABB AC500 PLC uses the CoDeSys Webserver.

ABB has produced a patch for the AC500 PLC that mitigates this vulnerability. This vulnerability affects multiple sectors to include the energy, critical manufacturing, and transportation sectors.

This vulnerability could be exploited remotely. Exploits that target this vulnerability are known to be publicly available.

AFFECTED PRODUCTS

The following ABB AC500 CPU modules with firmware Version V2.1.3 and Web server enabled are affected:

- 1SAP130 300 R0271 PM573-ETH,
- 1SAP140 300 R0271 PM583-ETH,
- 1SAP150 000 R0271 PM590-ETH,
- 1SAP150 100 R0271 PM591-ETH,
- 1SAP150 200 R0271 PM592-ETH,
- 1TNE968 900 R0110 PM554-T-ETH,
- 1TNE968 900 R1110 PM564-T-ETH,
- 1TNE968 900 R1210 PM564-R-ETH, and
- 1TNE968 900 R1211 PM564-R-ETH-AC.

a. ICSA-12-006-01 – 3S Smart Software Solutions CoDeSys Vulnerabilities, www.us-cert.gov/control_systems/pdf/ICSA-12-006-01.pdf, Web site last accessed November 15, 2012.

IMPACT

Exploitation of this buffer overflow vulnerability in the embedded CoDeSys Web server component used by ABB causes a DoS of the PLC that can only be recovered after cycling the system's power.

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 operational environment, architecture, and product implementation.

BACKGROUND

ABB is a Swiss-based company that maintains offices in several countries around the world. ABB develops products in multiple critical sectors that are deployed worldwide.

The affected products, AC500 PLCs, are Web-based SCADA systems. According to ABB, the AC500 PLCs are deployed across several sectors including the energy, critical manufacturing, transportation, and others. ABB estimates that these products are deployed worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

STACK-BASED BUFFER OVERFLOW[b]

The ABB AC500 Webserver uses the CoDeSys embedded software. By sending an overly long URL to Port 80/TCP (Port 80 by default, but the device may be configured to use any arbitrary port), an attacker could cause a stack-based buffer overflow. This causes a crash of the PLC. The only remediation is to cycle the system's power.

CVE-2011-5007[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[d]

b. CWE, http://cwe.mitre.org/data/definitions/121.html, CWE-121: Stack-Based Buffer Overflow, Web site last accessed November 15, 2012.

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5007 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C), Web site last accessed November 15, 2012.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

ABB has released a Vulnerability Security Advisory[e] and patch (V2.1.5) that mitigates this vulnerability that was made available in December 2011. Firmware versions starting from V2.1.4 do not contain the vulnerability. Firmware V2.1.5 can be found in the ABB PLC download center.[f]

The Web server component is not active in the default configuration of the system. It should only be used if human-machine interface visualization is required. PLCs that are continuously running are expected to be in a factory environment where additional cybersecurity measures, such as isolation, intrusion detection, etc., are part of normal security operations and reduce the risk for malware or unauthorized personnel to have a network connection to the PLC.

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.

e. ABB Vulnerability Security Advisory, http://www05.abb.com/global/scot/scot209.nsf/veritydisplay/e60fef809ebc595fc12579ea002f6d7d/$file/ABB%20Advisory%20ABBVU-DMLD-AC500CPUFW-1386.pdf, Web site last accessed November 15, 2012.

f . ABB PLC Download Center, http://www.abb.com/plc, Web site last accessed November 15, 2012.

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

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[h] that is available for download from the ICS-CERT Web page (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.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585

For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed November 15, 2012.

h. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed November 15, 2012.

development of proper mitigations may put industrial control systems and the public at avoidable risk.