ABB-VU-DMLD-AC500CPUFW-1386: Advisory for AC500 webserver

Overview

ABB is aware of a buffer overflow vulnerability in the webserver component of the AC500 PLC. Affected customers were informed by their local sales units after a patch was made available in December of 2011. This advisory completes the publication process.

CVSS Overall Score: 6.4
CVSS Vector: AV:N;AC:L;Au:N;A:C;I:N;C:N;E:F;RL:OF;RC:C

Affected Products

All AC500 CPU modules with firmware version **V2.1.3 and enabled** webserver:

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
1TNE968 900 R1211	PM564-R-ETH-AC

Impact

An attacker might use the vulnerability to cause a denial-of-service of the affected PLC by crashing the device. Only a power cycle will recover the device functionality.

Background

AC500 is a modular PLC platform that is used in a multitude of automation applications. The newer generation CPU modules use Ethernet and a number of protocols for communication with different services on the network. The webserver module supports clients with a way to connect to a customized HMI-type visualization by using a standard web browser.
In the default configuration, the webserver is **not** active.

Vulnerability Detail

The vulnerability originates from a buffer overflow in the webserver component when processing incoming requests from a client.

Exploitability

By using a specially crafted packet, an attacker can cause the webserver component to overwrite memory, resulting in a crash of the PLC and thus a denial-of-service of the PLC in question.

Existence of Exploit

A denial-of-service exploit has been demonstrated.

Mitigating Factors

The webserver component is not active in the default configuration and should only be used on systems that need an HMI visualization. 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.

Mitigation

ABB recommends to patch affected systems as described below.

Solution

All AC500 CPU firmware versions starting from V2.1.4 do not contain the vulnerability. The latest firmware version is always available at http://www.abb.com/plc in the download center.
The following link leads directly to the current firmware as of writing (V2.1.5):
http://search.abb.com/library/Download.aspx?DocumentID=1SAP190800R0215&LanguageCode=en&DocumentPartId=&Action=Launch

Acknowledgement

ABB would like to acknowledge Luigi Auriemma for finding the original bug in the CoDeSys webserver component (ICS-ALERT-11-336-01).
Further investigation and follow up by ABB revealed that contrary to the vulnerability of the PC version of the webserver, the PLC version does **not** allow injected code to be executed.

Contact

ABB customers using the AC500 PLCs integrated webserver component may contact their local sales units for further information, see www.abb.com.
For cyber security related questions, please contact cybersecurity@ch.abb.com

Further Information

This document and ABB information on cybersecurity can be found at:
www.abb.com/cybersecurity

Disclaimer