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:

<table>
<thead>
<tr>
<th>Model</th>
<th>Version</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>1SAP130</td>
<td>300</td>
<td>R0271 PM573-ETH</td>
</tr>
<tr>
<td>1SAP140</td>
<td>300</td>
<td>R0271 PM583-ETH</td>
</tr>
<tr>
<td>1SAP150</td>
<td>000</td>
<td>R0271 PM590-ETH</td>
</tr>
<tr>
<td>1SAP150</td>
<td>100</td>
<td>R0271 PM591-ETH</td>
</tr>
<tr>
<td>1SAP150</td>
<td>200</td>
<td>R0271 PM592-ETH</td>
</tr>
<tr>
<td>1TNE968</td>
<td>900</td>
<td>R0110 PM554-T-ETH</td>
</tr>
<tr>
<td>1TNE968</td>
<td>900</td>
<td>R1110 PM564-T-ETH</td>
</tr>
<tr>
<td>1TNE968</td>
<td>900</td>
<td>R1210 PM564-R-ETH</td>
</tr>
<tr>
<td>1TNE968</td>
<td>900</td>
<td>R1211 PM564-R-ETH-AC</td>
</tr>
</tbody>
</table>

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):

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
The information in this document is subject to change without notice, and should not be construed as a commitment by ABB. ABB provides no warranty, express or implied, for the information contained in this document, and assumes no responsibility for the information contained in this document or for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.