Remote code execution vulnerability in CAP 501/CAP 505/SMS 510 wserver.exe

ABB-VU-PPMV-1MRS757865

Notice

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, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

CAP 501 2.2.0, 2.3.0 and 2.4.0
CAP 505 2.2.0, 2.3.0 and 2.4.0
SMS 510 1.1.0, 1.2.0 and 1.3.0

Summary

A resolution is available that addresses a privately reported vulnerability affecting the product versions listed above. The vulnerability has been reported by ZDI (http://www.zerodayinitiative.com/) for CAP 501 version 2.4.0.

A vulnerability exists in the wserver.exe program included in the affected product versions. An attacker could exploit this vulnerability and run arbitrary code in order to e.g. cause the product to stop working or change the behavior of the product. The wserver.exe program is designed to allow remote execution of local programs but can also be mis-used for malicious tasks.

The vulnerability can be resolved by removing the vulnerable executable from the affected product installations or by using newer product versions.

Severity rating

The severity rating for this vulnerability is Moderate, with the overall CVSS score 5.9 (See http://www.first.org/cvss/cvss-guide.html for more information about the CVSS score). This assessment is based on the types of systems that are affected by the vulnerability, how difficult it is to exploit, and the effect that a successful attack exploiting the vulnerability could have.

CVSS Overall Score: 5.9

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P/E:P/RL:O/RC:C

CVSS Link: http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:P/A:P/E:P/RL:O/RC:C)

Corrective Action or Resolution

The resolution is the same for all the affected products. CAP 501 is replaced by the CAP 505 2.5.0 and all versions of CAP 505 (version 2.5 and later) do not have this vulnerability and SMS 510 is nowadays replaced by PCM600

The vulnerability is exposed when the wserver.exe program is running.

The wserver.exe program is used to launch the disturbance file Evaluation Tool in the DR-Collector Tool. The wserver.exe program is typically running only while there is an active Windows user session having wserver.exe in the Start-up folder of the Windows user.

Resolution

a. Disable the startup by removing wserver.exe shortcut from the start-up menu in Windows (Start > Programs > Startup)
b. Kill the wserver.exe process
c. Remove the file sc\prog\exec\wserver.exe from the computer file system

After this the user will no longer be able to directly start the Evaluation Tool from CAP 501/CAP 505/SMS 510, but will have to manually start the tool from Windows Start menu.

ABB recommends that customers apply the corrective actions at earliest convenience.

Vulnerability Details

A vulnerability exists in the wserver.exe program included in the product versions listed above. An attacker could exploit this vulnerability and run arbitrary code in order to e.g. cause the product to stop working or change the behavior of the product. The wserver.exe program is designed to allow remote execution of local programs but can also be mis-used for malicious tasks.
The vulnerability is caused by wserver.exe program accepting remote execution calls without proper user authentication. The wserver.exe program also has a buffer overflow vulnerability that can be used to execute arbitrary code on the destination computer.

Mitigating Factors

Recommended security practices and firewall configurations can help protect the control system from the attacks originated from outside the network. Such practices include that the control systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case. Control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to the control system.

More specific mitigation practices are described in the Corrective Actions or Resolution chapter above.

Workarounds

Workarounds are described in the Corrective Actions or Resolution chapter above.

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could start programs, delete files and kill processes etc. on the computer where the wserver.exe program is running.

What causes the vulnerability?
The vulnerability is caused by wserver.exe program accepting remote execution calls without a proper user authentication. The wserver.exe program also has a buffer overflow vulnerability that can be used to execute arbitrary code on the destination computer.

What is the wserver.exe?
The wserver.exe program is used to start the Evaluation Tool in the DR-Collector Tool from CAP 501/CAP 505/SMS 510. The wserver.exe program is typically running only while there is an active Windows user session having wserver.exe in the Start-up folder of the Windows user.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could start programs, delete files and kill processes, etc. on the computer where the wserver.exe program is running.

How could an attacker exploit the vulnerability?
An attacker could exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see the chapter Mitigating Factors above.

Could the vulnerability be exploited remotely?
Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that the control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

When this security advisory was issued, had this vulnerability been publicly disclosed?
No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?
No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- Andrea Micalizzi (aka rgod) of HP's Zero Day Initiative for Remote Code Execution Vulnerability (ZDI-CAN-1772)
- Brian Gorenc of HP's Zero Day Initiative for Remote Code Execution Vulnerability (ZDI-CAN-1785)

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

Information about ABB’s cyber security program and capabilities can be found at www.abb.com/cybersecurity.