Remote code execution vulnerabilities in MicroSCADA wserver.exe program

ABB-VU-PSAC-1MRS235805

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.

Affected Products

MicroSCADA, COM 500 4.1, 4.2
MicroSCADA, SYS 500 8.4.5
MicroSCADA Pro, SYS 600 9.0, 9.1, 9.1.5, 9.2, 9.3, 9.3 FP1, 9.3 FP2

Summary

A resolution is available that addresses two privately reported vulnerabilities affecting the product versions listed above. The vulnerability has been reported by ZDI (http://www.zerodayinitiative.com/). The vulnerabilities exists in the wserver.exe program included in the affected product versions. An attacker could exploit these vulnerabilities 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 vulnerabilities can be resolved by protecting the system from external network access or removing the vulnerable executable from the affected product installations. Newer product

versions (released after April 2013) will not contain the wserver.exe program and will therefore not have these vulnerabilities.

Severity rating

The severity rating for these vulnerabilities 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 vulnerabilities, how difficult they are to exploit, and the effect that a successful attack exploiting the vulnerabilities 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. SYS 500 and COM 500 are nowadays replaced by SYS 600 and all versions of SYS 600 starting with 9.4 and later do not have these vulnerabilities as the functionality is replaced with another solution.

The vulnerabilities are exposed when the wserver.exe program is running.

The wserver.exe program is used mainly in Workstation computers and primarily with the Classic Workplaces (Monitors of Type X or VS Remote). The wserver.exe program is used by the SCIL function WORKSTATION_CALL to allow a SCIL program to execute some program on the Workstation computer for example to sound some alarm or print a document. The wserver.exe program is typically running only while there is an active Windows user session having wserver.exe program in the Start-up folder of the Windows user.

Use cases and resolution

1. The wserver.exe program is running on the SYS 500/SYS 600/COM 500 server computer

The wserver.exe program is not needed on the server computer. If it is running on the server computer take the following actions:

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

2. The wserver.exe program is running on the workstation computer but is not used

The need for the wserver.exe program in the workstation can be checked by searching for WORKSTATION_CALL SCIL functions in the SCIL programs and pictures of the application. If it is not found the wserver.exe program is not needed. If it is found, check if it is still used.
If it can be concluded that WORKSTATION_CALL is not used and hence the wserver.exe program is not needed, take the following actions:

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

3. The wserver.exe program is running on the workstation computer and is used

If the wserver.exe program is running on the workstation and is still used there are two resolution alternatives:

1. Remove the need for the weserver.exe program by migrating the classic Workplaces to the newer Monitor Pro solution. If this can be done, continue the resolution according to scenario 2 where the wserver.exe program is no longer used.
2. The system should be protected from un-authorized access. This can be done in one or several of the following ways:

   a. Make sure that the system is not connected to external networks/internet
   b. Enable / configure a firewall for the workstation computer where the wserver.exe program is running. The firewall should be configured to only allow the SYS 500/COM 500/SYS 600 server to access the port 12221. The computer can either be protected by an external firewall that protects the whole network perimeter or by an integrated firewall for the computer in question only.

ABB recommends that customers apply the corrective actions at earliest convenience. Please contact your local ABB representative for more guidance if needed.

Vulnerability Details

A vulnerabilities exists in the wserver.exe program included in the product versions listed above. An attacker could exploit these vulnerabilities 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.
One vulnerability is caused by the wserver.exe program accepting remote execution calls without proper user authentication. The other vulnerability is caused by the wserver.exe program having a buffer overflow fault 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 attacks originating 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 vulnerabilities?
An attacker who successfully exploits these vulnerabilities could start programs, delete files and kill processes etc. on the computer where the wserver.exe program is running.

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

What is the wserver.exe program?
The wserver.exe program is used mainly in Workstation computers and primarily with the Classic Workstation (Monitors of Type X or VS Remote). The wserver.exe program is used by the SCIL function WORKSTATION_CALL to allow a SCIL program to execute some programs on the Workstation computer for example to sound some alarm or print a document. The wserver.exe program is typically running only while there is an active Windows user session having a shortcut to the wserver.exe program in the Start-up folder of the Windows user.

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

How could an attacker exploit these vulnerabilities?
An attacker could exploit the vulnerabilities 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 vulnerabilities be exploited remotely?
Yes, an attacker who has network access to an affected system node could exploit these vulnerabilities. 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 these vulnerabilities been publicly disclosed?
No, ABB received information about these vulnerabilities through responsible disclosure.

When this security advisory was issued, had ABB received any reports that these vulnerabilities were being exploited?
No, ABB had not received any information indicating that these vulnerabilities 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.