ABB-VU-DMRO-41532: Advisory for WebWare Components and Related Products

Overview

The legacy PC products WebWare Server, WebWare SDK and other legacy products that include parts of WebWare contain a number of COM and ActiveX components. These components have been found to contain a potential vulnerability with regards to the COM interfaces and the scripting interfaces on these components.

CVSS Overall Score: 7.7

Affected Products

WebWare Server:	All versions of included Data Collector and Interlink
WebWare SDK:	All versions
ABB Interlink Module:	All versions
S4 OPC Server	All versions
QuickTeach	All versions
RobotStudio S4	All versions
RobotStudio Lite	All versions

Impact

An attacker, with knowledge of the PC running the above products and components could potentially use the COM and scripting vulnerabilities to deny service for the application, to elevate their execution privilege on the PC, or allow an attacker to run remote code on the PC.

Background

The WebWare software products include a number of COM and ActiveX controls. These controls are delivered and installed together in the above products. The purpose of these controls is to facilitate communications with the robot controller or the WebWare Server and may run as a service on the PC. Other controls provide graphical elements for web pages and custom HMI's.

The above products are used in several different roles in a factory environment. WebWare Server is used for data gathering and backup handling; WebWare SDK, ABB Interlink Module, and S4 OPC Server are used for HMI's and communications to and from a robot controller. QuickTeach, RobotStudio S4, and RobotStudio Lite are PC tools used for training, installation, and programming of a robot cell.

Vulnerability Detail

The COM and ActiveX controls included in the software do not have complete checks on all possible bad input data. This implies that a user or program could call one of the controls' interfaces with specially crafted input data which overflows the stack pointer or causes the control to stop execution. The ActiveX controls have been registered as scriptable, which means that they can be included and scripted from web pages served remotely.

Exploitability
Attackers with access to the machine could attack the COM interfaces of the controls with bad input data to cause the underlying services to stop execution, denying service. If the machine has a developer license, then an attacker with access to the machine could use the vulnerability to raise their privilege to the level of the service or program running the controls; in some installations the default level is Administrator.

If an attacker can get a user on the machine to visit their malicious web site, then they can potentially build web pages that reference the WebWare ActiveX controls and use scripts to attack the ActiveX controls' interfaces and could potentially enable remote execution of code running in the browser space.

Existence of Exploit
There is no exploit code publicly available.

Mitigating Factors
WebWare Server and Web Ware components were tools for older Windows operating systems: Windows XP and Windows 2003 Server. As these operating systems are nearing the end of the Microsoft security support cycle, responsible users continuing to use these operating systems should be preparing measures for ensuring cyber security of the operating system itself. These measures will of themselves mitigate the risk to the WebWare components.

Mitigation
In general, good cyber security practices mitigate the risk. Information on good practices for Webware server and WebWare components can be found in the publication SI10231A1 "WebWare Component Security".

Solution
WebWare Server, and the above products are legacy PC products nearing the end of their lifecycle and are no longer actively developed. Users of these products are directed to the available documentation on mitigating risk and securing their machines and production environments.

Acknowledgement
ABB would like to acknowledge the work of Billy Rios, Terry McCorkle and the ICS-CERT team for first reporting this in WebWare Server 4.91.

Further investigation and followup by ABB revealed other legacy products affected by this vulnerability.

Contact

ABB customers using these products may contact their local ABB Robotics service organization, see www.abb.com for information.

Questions or responses on Cyber Security may be addressed to: cybersecurity@ch.abb.com

Further Information

This document and ABB information on Cyber Security can be found at: www.abbb.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.