Advisory for Test Signal Viewer for Robotics

ABBVU-DMRO-53125

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

Test Signal Viewer	all versions up to version 1.4

Summary

Test Signal Viewer is a PC product used to tune and adjust external axes and robot axes in the IRC5 controller.
The product is normally distributed on the RobotWare 5.05 – 5.15 DVD that accompanies the IRC5 controller.

A vulnerability exists in a 3rd party component installed with the Test Signal Viewer Windows PC program. Using this vulnerability, and by getting the PC user to surf to a specially crafted web site, an attacker could gain control over the PC. A new version of Test Signal Viewer, Version 1.5 has been released to address this vulnerability.

Severity rating

The severity rating for this vulnerability is Low, with the overall CVSS score 6.5. 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: 6.5

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

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

Corrective Action or Resolution

The problem is corrected in the following product version:

Test Signal Viewer version 1.5

This version is available for download on ABB Library, under **SI10253** as well as found in the RobotWare 5.15.03 and 5.60 DVD.

ABB recommends that customers apply the update at earliest convenience

Vulnerability Details

The vulnerability originates from a 3rd party component that was installed together with Test Signal Viewer. An attacker, wishing to take over the PC running Test Signal Viewer would need to build a specially crafted website and get the PC user to open the site in their web browser. This would allow the attacker to utilize the vulnerability in the 3rd party component to install arbitrary code on the PC and gain control over the PC.

Mitigating Factors

Use of web browsers and antivirus programs that check and report on phishing sites or suspicious web sites will help to mitigate the risk.

Workarounds

a) Uninstall Test Signal Viewer when it is no longer needed,

b) Disable ActiveX controls in the web browser,

Frequently asked questions

What is the scope of the vulnerability?
An attacker who successfully exploited this vulnerability could take control of an affected system and run arbitrary code in an affected system.

What causes the vulnerability?

The vulnerability is caused by incorrect control of input data in a 3rd party ActiveX component that was installed together with Test Signal Viewer. This 3rd party component was marked “safe for scripting” allowing it to be used in web pages.

What is the affected component?
The affected 3rd party component was included in the installation as a convenience and was not used by Test Signal Viewer.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability would be able to insert arbitrary files on the user’s disk drive with the potential of inserting code to be run at startup.

How could an attacker exploit the vulnerability?
An attacker could try to exploit the vulnerability by creating a specially crafted website with web pages that activate the 3rd party component invisibly to the user. The attacker could then script commands in the web page that load data via the component to the user’s hard disk.
Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?
Yes, but only if the user of the Windows PC visits a malicious website that was setup to exploit this vulnerability.

What does the update do?
The update removes the vulnerability by updating the 3rd party component that has been changed by its manufacturer to remove the vulnerability.

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 for discovering this vulnerability and working with TippingPoint's Zero Day Initiative,
- The Zero Day Initiative for forwarding the reported vulnerability description to ABB.

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.