Advisory for ABB RobotStudio

ABB-VU-DMRO-13944

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

ABB RobotStudio from version 5.06 up to and including version 5.61.01.01

Summary

The RobotStudio software is a PC product used for offline programming and simulation of ABB Robot system. The vulnerability exists in an executable file included in the product versions listed above.

An update is available that resolves the privately reported vulnerability in the product versions listed above. The vulnerability could allow an attacker who successfully exploited this vulnerability to insert and run arbitrary code on an affected system.

Severity rating

The severity rating for this vulnerability is Moderate; with the overall CVSS score 6.9. 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: 6.9

CVSS Vector: *AV:L/AC:M/Au:N/C:C/I:C/A:C/E:ND/RL:ND/RC:ND*

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

Corrective Action or Resolution

The problem is corrected in the following product version:

RobotStudio version 5.61.02

This version is available for download at RobotStudio download page at the following hyperlink: http://new.abb.com/products/robotics/robotstudio/downloads

ABB recommends that customers apply the update at earliest convenience.

Vulnerability Details

A vulnerability exists in a third-party component included in the product versions listed above. Specifically the vulnerability is in an executable that is executed during installation of the product.

The vulnerability can be exploited when the executable file is executed during installation of RobotStudio to resolve the location of other DLLs to be dynamically loaded by a third-party component. The executable file has mistakenly been included, but not used, in the distribution of all RobotStudio versions from 5.60 up to and including 5.61.01.01.

An attacker could exploit the vulnerability by inserting and run arbitrary code. The victim has to interact with an untrusted source.

Mitigating Factors

For an attack to be successful, a user must visit an untrusted remote file system location and open a document from this location.

Use of web browser and antivirus program that check and report on phishing sites or suspicious web sites will help to mitigate the risk. Removable storage media should be carefully scanned for viruses before they are used.

Workarounds

ABB has not identified any workaround for this vulnerability.

Frequently asked questions

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

What causes the vulnerability?
The vulnerability is caused by RobotStudio loading Dynamic Link Libraries (DLLs) from insecure file location.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could gain the same user rights as a logged-on user. If the user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take full control of an affected system and make unauthorized changes to the system.

How could an attacker exploit the vulnerability?
To exploit this vulnerability, an attacker could use an untrusted source to deliver the specifically crafted DLL file to the victim's computer.

Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?
No, to exploit this vulnerability an attacker would need to have physical access to an affected system or convinces the victim on the computer to interact with an untrusted source such as a remote network location.

What does the update do?
The update removes the vulnerable executable file.

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:

- Ivan Sanchez of WiseSecurity Team for discovering this vulnerability and bringing the incident to our attention and working with us on the response.

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.