ABB-VU-DMRO-38599: Buffer Overflow in Robot Communications Runtime on Windows

Overview

A buffer overflow exists in a component of the Robot Communication Runtime used on Windows PC's in the communications to the IRC5, IRC5C, and IRC5P robot controllers.

CVSS Overall Score: 10.0

Affected Products

RobotStudio:	Versions supporting IRC5 up to and including 5.14.01
Robot Communications Runtime:	Versions up to and including 5.14.01
PickMaster 3:	Versions up to and including 3.3
PickMaster 5:	Versions up to and including 5.13
RobView 5:	*Works together with other products listed here.*
PC SDK:	Versions up to and including 5.14.01
IRC5 OPC Server:	Versions up to and including 5.14.01
WebWare SDK:	Versions 4.6 through 4.9
ABB Interlink Module:	Versions 4.6 through 4.9
WebWare Server:	Versions 4.6 through 4.91

Impact

A dedicated attacker might be able to use this vulnerability to cause a denial-of-service for the robot scanning and discovery service on the PC and potentially remotely execute code on the Windows PC. Depending upon the installation, the remote code execution could run with administrator privilege.

Background

Products such as RobotStudio and PickMaster 5 are used in installation, programming, and commissioning of an ABB industrial robot. Products such as PickMaster 3, IRC5 OPC Server, WebWare SDK are used for continuous operations and custom HMIs for Windows PC's connected to the robot controller over a factory network.

Vulnerability Detail

The vulnerability originates from a buffer overflow in the RobNetScanHost service component when processing incoming announcements on robot controller availability on the subnet.

Exploitability

By using a specially crafted packet, an attacker can cause the RobNetScanHost service to terminate, resulting in a denial-of-service for finding robot controllers on the network. A dedicated attacker might be able to use the buffer overflow to download and execute code on the affected PC..

Existence of Exploit
A denial-of-service exploit has been demonstrated.

Mitigating Factors
The RobNetScan host service is only running when a client is active on the Windows machine. Clients that are continuously running are expected to be in an factory environment where additional cyber security measures, such as isolation, intrusion detection, etc, are part of normal security operations and reduce the risk for malware or unauthorized personnel to have a network connection to the Windows machine.

Mitigation
ABB recommends to apply the solution as described below.

Solution
All of the 5.14.02 and above versions of RobotStudio, PC SDK, and IRC5 OPC Server do not have the vulnerability and will correct any existing installations.
PickMaster 3 version 3.40 and PickMaster 5 version 5.20 and future versions are also updated and will correct any existing installation.
The RobotWare 5.14.02 release DVD contains an updated Robot Communications Runtime 5.14.02 and installing this version will correct all products on the PC.
RobView 5 can be updated by installing any new product from the list above or using the available patch.

For existing installations or for products that are not immediately corrected, a service patch: "ABB Robot Communications Runtime Patch 38599.msi" is available under the link >>
Security Patch for Robot Communication Runtime on Windows: ABBVU-DMRO-38599**.**

Acknowledgement
ABB would like to acknowledge Luigi Auriemma and Tipping Point ZDI (ZDI-CAN-1260) for first reporting this for WebWare Server 4.91.

Further investigation and followup by ABB revealed more 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.abb.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.