Multiple Vulnerabilities in ABB RobotWare

ABB-VU-DMRO-124641, ABB-VU-DMRO-124642,
ABB-VU-DMRO-124644, ABB-VU-DMRO-124645,
ABB-VU-DMRO-128238

Update Date: 2016-11-11

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

RobotWare 5.x	(any version prior to 5.15.13)
RobotWare 5.6x	(any version prior to 5.61.07)
RobotWare 6.x	(any version prior to 6.04.00)

Summary

ABB is aware of four privately reported vulnerabilities in RobotWare versions listed above. Updates are available that resolves all reported vulnerabilities.

a. ABBVU-DMRO-124641: Buffer overflow leading to arbitrary remote code execution
b. ABBVU-DMRO-124642: Remote command execution
c. ABBVU-DMRO-124644: Authentication bypass

d. ABBVU-DMRO-124645: Buffer overflow in FlexPendant

e. ABBVU-DMRO-128238 Remote buffer overflow in command endpoint

An attacker who successfully exploited these vulnerabilities could cause the robot controller to stop, make the robot controller inaccessible, take remote control of the robot controller, or insert and run arbitrary code.

Vulnerability Severity

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both CVSS v2 and v3. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

ABBVU-DMRO-124641: Buffer overflow leading to arbitrary remote code execution

CVSS v2 Base Score: 9.3

CVSS v2 Temporal Score: 7.7

CVSS v2 Vector: *AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C*

CVSS v2 Link: http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

CVSS v3 Base Score: 8.1 (High)

CVSS v3 Temporal Score: 7.5 (High)

CVSS v3 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

ABBVU-DMRO- 124642: Remote command execution

CVSS v2 Base Score: 8.5

CVSS v2 Temporal Score: 7.0

CVSS v2 Vector: *AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C*

CVSS v2 Link:
http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C)

CVSS v3 Base Score: 7.5 (High)
CVSS v3 Temporal Score: 7.0 (High)
CVSS v3 Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v3 Link:
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

ABBVU-DMRO- 124644: Authentication bypass

CVSS v2 Base Score: 9.3
CVSS v2 Temporal Score: 7.7
CVSS v2 Vector: *AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C*
CVSS v2 Link:
http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

CVSS v3 Base Score: 8.1 (High)
CVSS v3 Temporal Score: 7.5 (High)
CVSS v3 Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v3 Link:
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

ABBVU-DMRO-124645: Buffer overflow in FlexPendant

CVSS v2 Base Score: 4.3
CVSS v2 Temporal Score: 3.2
CVSS v2 Vector: *AV:A/AC:H/Au:N/C:P/I:P/A:P/E:U/RL:OF/RC:C*
CVSS v2 Link:
http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:A/AC:H/Au:N/C:P/I:P/A:P/E:U/RL:OF/RC:C)

CVSS v3 Base Score: 5.0 (Medium)
CVSS v3 Temporal Score: 4.4 (Medium)
CVSS v3 Vector: AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C
CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:U/RL:O/RC:C

ABBVU-DMRO-128238 Remote buffer overflow in command endpoint

CVSS v2 Base Score: 7.5
CVSS v2 Temporal Score: 5.5
CVSS v2 Vector: AV:N/AC:M/Au:S/C:P/I:P/A:C/E:U/RL:OF/RC:C
CVSS v2 Link: http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:S/C:P/I:P/A:C/E:U/RL:OF/RC:C)

CVSS v3 Base Score: 6.4 (Medium)
CVSS v3 Temporal Score: 5.6 (Medium)
CVSS v3 Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C
CVSS v3 Link: https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C

Corrective Action or Resolution

The problems are corrected in the following product versions:

RobotWare version 5.15.13
RobotWare version 5.61.07
RobotWare version 6.04.00

The updates are available for download from within RobotStudio.

ABB recommends that customers apply the suitable update at earliest convenience.

Vulnerability Details

ABBVU-DMRO-124641: Buffer overflow leading to arbitrary remote code execution

A buffer overflow vulnerability exists in Robot Communication server running on main computer in the RobotWare versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the robot controller and insert and run arbitrary code.

ABBVU-DMRO- 124642: Remote command execution

A vulnerability exists in the main computer in the RobotWare versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the robot controller and invoke and run arbitrary commands.

ABBVU-DMRO- 124644: Authentication bypass

A vulnerability exists in the main computer in the RobotWare versions 5.x. An attacker who exploit this vulnerability can gain access to the robot controller without authentication.

ABB has not being able to fully resolve this vulnerability in RobotWare version 5.x. The vulnerability still exists for the Service port. Recommended practices to reduce the risks of this vulnerability is found in the section Mitigating Factors below.

ABBVU-DMRO-124645: Buffer overflow in FlexPendant

A vulnerability exists in the FlexPendant in the product versions listed above. An attacker could exploit the vulnerability by a specially crafted message to the FlexPendant and allowing the attacker to insert and run arbitrary code on the FlexPendant.

ABBVU-DMRO-128238 Remote buffer overflow in command endpoint

A buffer overflow vulnerability exists in the main computer in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the robot controller and insert and run arbitrary code.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a robot controller from attacks that originate from outside the network. Such practices include that robot controllers are physically protected from direct access by unauthorized personnel, have no access from 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. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to the robot controller.

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 these vulnerabilities could prevent legitimate access to an affected robot controller, remotely cause an affected robot controller to stop, and insert and run arbitrary code.

What causes the vulnerability?
Some of the vulnerabilities are caused by unchecked buffers / unchecked input data in the main computer and in the FlexPendant.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could cause the affected robot controller to stop or become inaccessible. An attacker can take control of the robot controller by inserting and running arbitrary code.

How could an attacker exploit the vulnerability?
An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected robot controller. This would require that the attacker has access to the network of the robot controller, by connecting to the network either directly or through a wrongly configured or penetrated firewall or infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?
Yes, an attacker who has network access to an affected robot controller could exploit this vulnerability. Recommended practices include that robot control systems are physically protected, have no access from Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?
The update removes the vulnerabilities by modifying the way RobotWare validates messages, authenticates users and verify input data.

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:

- Davide Quarta, Marcello Pogliani, Mario Polino, Stefano Zanero and Federico Maggi from Politecnico di Milano for discovering these vulnerabilities and bringing the incidents 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.