DOCUMENT ID: SI20330
REVISION: A
DATE: 2024-05-14

CYBER SECURITY ADVISORY

IRC5 / OmniCore RobotWare – Multiple Vulnerabilities

CVE ID: CVE-2024-1913, CVE-2024-1914

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.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

Platform	Product	Version
IRC5	RobotWare 6	< 6.15.06 except 6.10.10, and 6.13.07
OmniCore	RobotWare 7	< 7.14

Vulnerability IDs

CVE-2024-1913, CVE-2024-1914

Summary

Updates are available that resolves privately reported vulnerabilities in the RobotWare versions listed above.

An attacker who successfully exploited these vulnerabilities could cause the robot to stop, make the robot controller inaccessible, or execute arbitrary code.

Recommended immediate actions

The vulnerabilities are corrected in the following RobotWare versions:

RobotWare 6.10.10, 6.13.07, 6.15.06, and 7.14

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

The vulnerabilities exist in the Robot Web Services in the RobotWare versions listed above. An attacker could exploit the vulnerabilities by sending specially crafted messages to the robot controller, causing the robot to stop, become inaccessible, or execute arbitrary code.

It is important to note that for an attacker to exploit these vulnerabilities, they must first be authenticated within the system. This requirement signifies that the potential exploit is not immediately accessible to arbitrary external attackers but rather poses a risk in scenarios where an authenticated user attempts to exploit their existing privileges for unauthorized purposes.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2024-1913 Out-of-bounds write

The vulnerability could potentially be exploited to perform unauthorized actions by an attacker. This vulnerability arises under specific condition when specially crafted message is processed by the system.

CVSS v3.1 Base Score:	7.6 (High)
CVSS v3.1 Temporal Score:	7.3 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:H/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-1913

CVE-2024-1914 Null pointer dereference

The vulnerability could potentially be exploited to perform unauthorized actions by an attacker. This vulnerability arises under specific condition when specially crafted message is processed by the system.

CVSS v3.1 Base Score:	6.5 (Medium)
CVSS v3.1 Temporal Score:	6.2 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:H/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-1914

Mitigating factors

Refer to section “General security recommendations” for further advise on how to keep your system secure.

[1] 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.

Workarounds

Although these workarounds will not correct the underlying vulnerability, they can help blocking or limiting known attack vectors:

- On OmniCore, use the internal firewall and disable Robot Web Services on the WAN port, or use an external firewall to block access to the network ports.
- On IRC5, use an external firewall to block access to the network ports.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited these vulnerabilities could remotely cause the robot controller to stop or execute arbitrary code.

What causes the vulnerabilities?

The vulnerabilities are caused by out-of-bounds write and null pointer dereference. The vulnerabilities arise under specific conditions when a specifically crafted messages are processed by the system.

What is RobotWare?

RobotWare is the software installed in the ABB robot controllers and designed to operate the robot.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the robot to stop, become inaccessible, or execute 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 the robot controller. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall. 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 the affected robot controller could exploit these vulnerabilities. It is important to note that for an attacker to exploit these vulnerabilities, they must first be authenticated within the system. This requirement signifies that the potential exploit is not immediately accessible to arbitrary external attackers but rather poses a risk in scenarios where an authenticated user attempts to exploit their existing privileges for unauthorized purposes.

What does the update do?

The update removes the vulnerabilities by modifying the way the robot controller validates messages and verify input data.

When this security advisory was issued, had these vulnerabilities been publicly disclosed?

No, ABB received information about these vulnerabilities through responsible disclosure.

When this security advisory was issued, had ABB received any reports that these vulnerabilities had been exploited?

No, ABB had not received any information indicating that these vulnerabilities had been exploited when this security advisory was originally issued.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Acknowledgement

ABB thanks Yuncheng Wang, Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China for responsibly reporting the vulnerabilities and working with us as we addressed them.

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2024-05-14