Vulnerabilities in SREA-01 and SREA-50 legacy Remote Monitoring Tools for Drives

ABBVU-RMDR-3AXD10000621970

Update Date: -

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

SREA-01 revisions A, B, C	application versions up to 3.31.5
SREA-50 revision A	application versions up to 3.32.8

Vulnerability ID

ABB ID: ABBVU-RMDR-3AXD10000621970

Summary

An update is available that resolves a publicly reported vulnerability in the products listed above. Products are based on legacy software platform which is no longer actively maintained.

An attacker who successfully exploited this vulnerability could access files on the affected products' file system without authorization, view data, change configuration, retrieve password hash codes and potentially insert and send commands to connected devices.

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.

CVSS v2 Base Score:	10.0
CVSS v2 Temporal Score:	8.3
CVSS v2 Vector:	*AV:N/AC:L/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:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

CVSS v3 Base Score:	9.8
CVSS v3 Temporal Score:	9.1
CVSS v3 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v3 Link:	http://nvd.nist.gov/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

Corrective Action or Resolution

The problem is corrected by installing a patch that is available at address (Link):

http://search-ext.abb.com/library/Download.aspx?DocumentID=9AKK107045A1782&LanguageCode=en&DocumentPartId=&Action=Launch

Note: ABB has tested the patch only with the latest revisions of the SREA-01 and the patch should be applicable also for the SREA-50. If an old revision of hardware is in use, it is suggested to replace the hardware either with latest revision or with some other Remote Monitoring tool.

Vulnerability Details

A vulnerability exists in the Netbiter software platform legacy version, included in the product versions listed above. There is an example code published in github by Bertin Jose and Fernandez Ezequiel.

By using the vulnerability, internal files of the above listed products can be accessed without any authorization over the network, using a HTTP request which refers to files using ../../ relative paths.

Once the internal password file is retrieved, the password hash can be identified using a brute force attack. There is also an exploit allowing running of commands after authorization.

Mitigating Factors

Recommended security practices and firewall configurations can help protect the Remote Monitoring Tools from attacks that originate from outside the network. Such practices include that Remote Monitoring tools are physically protected from direct access by unauthorized personnel, have no direct connections to the 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 should be carefully scanned for viruses before they are connected to the network.

VPN (Virtual Private Networking) access should be used to connect to the web interface of the SREA-01 module from further locations than the local network, as the web pages use unencrypted HTTP communication. The web interface of the SREA-01 and SREA-50 Remote Monitoring Tools should never be exposed directly to public Internet.

More information on recommended practices can be found in the following documents:

3AXD10000492137, Technical guide: Cybersecurity for ABB drives

Workarounds

In addition to the provided patch, the only known workarounds are:

- disconnecting the product from network entirely
- strictly firewalling network access to the web interface of the SREA-01 and SREA-50 HTTP ports (TCP ports 80 and 8080)

The web interface should be accessible only from trusted networks and devices.

Usage of VPN for remote access to the HTTP web interface is highly recommended.

It is also recommended to disable the secondary HTTP port (default TCP:8080) if that port is not needed.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could disclose password protected information, prevent legitimate access to an affected web interface, control devices, insert and run arbitrary code in an affected system node.

What causes the vulnerability?

The vulnerability is caused by unfiltered handling of malicious HTTP requests.

What is the SREA-01 / SREA-50?

SREA-01 is an Ethernet adapter / Remote Monitoring Tool for monitoring of selected Low Power Drives. It is based on legacy version of the HMS Netbiter platform. The product can be used also as generic Modbus/RTU and Modbus/TCP monitoring and control. Product is based on legacy software platform and largely replaced by other ABB Remote Monitoring Tools.

SREA-50 was a special variant targeted for monitoring of a PVS300 Solar inverter. Product has been switched to classic phase yr. 2013 and has limited availability.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could login to the device. As logged in user attacker could read and write information and run code.

How could an attacker exploit the vulnerability?

There is a publicly released sample code released by Bertin Jose and Fernandez Ezequiel.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the 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 vulnerability by improving message validation and user authentication. Patched product verifies input data more extensively than before the patch.

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

Yes, this vulnerability has been publicly disclosed.

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 specifically on SREA-01 or SREA-50 products when this security advisory was originally issued.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- Bertin Jose and Fernandez Ezequiel for finding the vulnerability
- HMS Industrial Networks Ab for providing a patch which corrects the issue

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.