DOCUMENT ID: 9AKK108468A4093
REVISION: A
DATE: 2023-07-14

CYBER SECURITY ADVISORY

AO-OPC Unquoted Service Path

CVE ID: CVE-2023-2685

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.

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

ABB has determined that all AO-OPC versions up to (including) 3.2.1.0 are affected.

Vulnerability IDs

CVE-2023-2685

Summary

A vulnerability was found in AO-OPC server versions mentioned above. As the directory information for the service entry is not enclosed in quotation marks, potential attackers could possibly call up another application than the AO-OPC server by starting the service. The service might be started with system user privileges which could cause a shift in user access privileges.

It is unlikely to exploit the vulnerability in well maintained Windows installations since the attacker would need write access to system folders.

An update is available that resolves the vulnerability found during an internal review in the product versions listed above.

Recommended immediate actions

The problem is corrected in the following product versions:

AO-OPC version 3.3.0

ABB recommends that customers apply the update at earliest convenience.

To obtain the installation files for the updated AO-OPC version please contact de-support.analytical@abb.com using the subject line “AO-OPC update”.

Alternatively, the steps below are recommended:

1. After each registration of AO-OPC as a service, start the registry editor (administrator privileges are needed)

2. Open the registry entry
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Optima OPC Service

3. Enclose the string value that is entered under "ImagePath" with quotation marks.
Example.: "C:\Program Files (x86)\Analyze IT\AO-OPC\OptimaOPC.exe"

Vulnerability severity and details

A vulnerability exists due to a lack of quotation marks in the registry entry containing the service path created upon installation of AO-OPC in the product versions listed above.

An attacker could exploit the vulnerability by using such a file as “C:\Program” to be started by AO-OPC. A shift in user privileges might be possible.

Please refer to CWE-428 Unquoted Search Path or Element for general information on this problem.

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

CVE-2023-2685

CVSS v3.1 Base Score:	7.2
CVSS v3.1 Temporal Score:	6.8
CVSS v3.1 Vector:	AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:F/RL:T/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-2685

[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.

Mitigating factors

To exploit the vulnerability an attacker would need access to the system, either physically or remotely through a wrongly configured or penetrated firewall and has writing rights to system folders. Additionally, knowledge about the presence of the vulnerability in AO-OPC is required. In well maintained Windows installations saving files to system folders is only possible with administrator privileges, reducing the chance of exploiting.

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

Workarounds

There are no workarounds needed as the vulnerability can be permanently fixed performing the recommended immediate actions.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploits this vulnerability could insert and run arbitrary code in an affected system node and cause a shift in user privileges.

What causes the vulnerability?

The vulnerability is caused by missing quotation marks in the service path registry entry.

What is AO-OPC?

The AO-OPC server allows connection of Advance Optima gas analyzers to any SCAD, DCS or PLC system which has an OPC client.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could allow the attacker to insert and run arbitrary code and shift user privileges.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by placing an executable file such “C:\Program” in the system and starting the AO-OPC service. The previously mentioned file would be executed instead of the AO-OPC server with the privileges granted to the service. This would require that the attacker has access to the system, either physically or remotely through a wrongly configured or penetrated firewall and has writing rights to system folders.

Recommended practices and well configured windows installations 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 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 adding the service paths missing quotation directly upon installation.

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.

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.
- Make sure that only users administration privileges are able to modify/add files to system folders.

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	05-12-23