9AKK107680A0672 TECHNICAL ANNOUNCEMENT

ABB Ability™ Operations Data Management zenon Vulnerability in ABB Ability™ ODM zenon editor

Introduction

ABB has received a report by Yongjun liu of nsfocus security team, detailing a security vulnerability in the COPA-DATA zenon editor software and the ABB Ability™ ODM zenon version of this software.

The COPA-DATA zenon editor software is used for creating and maintaining ABB Ability™ ODM zenon editor projects and for creating runtime files, which are used by ABB Ability™ ODM zenon runtime software.

Products affected

Systems where the ABB Ability™ ODM zenon editor is installed, are affected.

Versions affected

ABB Ability™ ODM zenon editor versions 8.00 SR1 (Build 57280) and older are affected.

Vulnerability details

CVE-2019-15638 - COPA-DATA zenone32.exe zenon editor uncontrolled search path vulnerability

CVSS v3 base score and vector:

A CVSS v3 base score of 7.8 has been calculated for this vulnerability. The corresponding CVSS v3 vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Additional information

The vulnerability is present on all systems with a vulnerable version of the ABB Ability™ ODM zenon editor installed. Under specific circumstances the ABB Ability™ ODM zenon editor may load dll files provided by an attacker from a directory for which no administrator rights are required for writing files and execute code of the attacker in the context of the user that started the ABB Ability™ ODM zenon editor

In order to exploit this vulnerability, an attacker needs to place a .wsp6 file and a malicious .dll file in a location accessible to the user and requires the user to use Windows explorer to explicitly open the .wsp6 file from this location. Systems with only the zenon runtime installed, are not affected.

Mitigations

Remove .wsp6 file type association
During installation of the ABB Ability™ ODM zenon editor, the file extension .wsp6 is registered to open with the ABB Ability™ ODM zenon editor application. Removing the association for the .wsp6 file type in Windows, prevents a user from opening such a file with the ABB Ability™ ODM zenon editor and prevents this vulnerability from being exploited.

Application Whitelisting
Application whitelisting is a technology that allows preparation of a Windows system, to allow execution only of trusted applications. These may include Windows components but also third party applications. Any executable file or dll file that is not explicitly defined on a whitelist, is prevented from being executed or loaded.

Application Whitelisting can be based on unique digital signatures (hashes) of applications, or digital issuer certificates, in combination with file version information and or file names. All COPA-DATA executable files are digitally signed by COPA-DATA. Making use of application whitelisting based on the COPA-DATA digital certificate, may allow installation of an official COPA-DATA update or patch, without the need to update the whitelist, and may also be able to prevent a downgrade to an older version.

Application Whitelisting can effectively prevent execution of malicious applications that are not trusted.

Processes and Procedures
Instruct users to open the ABB Ability™ ODM zenon editor application only through the Windows start menu or the ABB Ability™ ODM startup tool and not make use of the possibility to open .wsp6 files directly.

Patch Availability

COPA-DATA provides build updates for versions 7.50 and higher in which this issue is resolved. Users of older versions can perform an upgrade to a current version or use one of the mitigation options.

zenon version 7.50 build 61995

zenon version 7.60 build 61612

All ABB Ability™ ODM zenon versions higher than 7.60, which are downloadable from www.abb.com/zenon are not vulnerable.

Update

Recommendations
ABB recommends installing only the zenon runtime component on production systems and not the zenon editor.

ABB generally recommends using the ABB Ability™ ODM zenon editor on a separate engineering system in a protected environment to which access is restricted to authorized users only and on which appropriate security measures like the use of application whitelisting and antivirus software, are in place.

ABB recommends that system integrators and asset owners perform a risk assessment to establish whether the updated version of the ABB Ability™ ODM editor shall be installed.

ABB generally recommends keeping the operating system and software up to date.

ABB recommends testing the updated version of the ABB Ability™ ODM zenon software in a test environment to verify normal operation of the system according to project specific configuration and hardware environment, prior to installing the update in a production environment.

ABB recommends that a contingency plan is in place to roll back the installation of the update in case of any unexpected issues with the production environment following the installation of the patch.

Procedure
The process to install a build update is documented in the zenon online help in the chapter “Installation and updates” -> “Updates (Build Setup”

When the update is installed on the system with the zenon editor, it may also be necessary to update systems with the zenon runtime, when the project needs to be changed and changed runtime files need to be used on the runtime system.

General recommendations

ABB generally recommends restricting local physical access to authorized people only. Network access shall be limit to communication that is absolutely required.

Using VLANs and firewalls to segment network traffic and create zones and conduits, reduces exposure of systems in protected environments and allows network access to be restricted to only those systems or components that are in fact necessary.

ABB further recommends using application whitelisting to restrict execution of applications to only those trusted applications that are required for the operation of the system.

Acknowledgements

ABB wishes to thank Yongjun liu of nsfocus security team for disclosing this vulnerability responsibly and for the efforts taken in communication with ABB and its suppliers regarding the coordination of the publication of the vulnerability.

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers. Information about ABB's cyber security program and capabilities can be found at https://www.abb.com/cybersecurity.

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.