

Security Vulnerability Announcement 2019_5

Vulnerability in COPA-DATA zenon
editor

www.copadata.com
sales@copadata.com



zenon
by COPA-DATA

1. History

Date	Comment
05.09.2019	Created
23.10.2019	Patch availability version 8.10, 8.00
19.11.2019	Updated patch availability

Content

1. HISTORY	1
2. INTRODUCTION.....	3
3. PRODUCTS AFFECTED	3
4. VERSIONS AFFECTED	3
5. VULNERABILITY DETAILS	3
6. PATCH AVAILABILITY.....	5
7. UPDATE.....	5
Recommendations	5
Procedure	6
8. GENERAL RECOMMENDATIONS	6
9. ACKNOWLEDGEMENTS	6

2. Introduction

COPA-DATA has received a report by Yongjun liu of nsfocus security team, through a COPA-DATA OEM customer, detailing a security vulnerability in the COPA-DATA zenon editor software and OEM versions of this software.

The COPA-DATA zenon editor software is used for creating and maintaining zenon editor projects and for creating runtime files, which are used by the independent COPA-DATA zenon runtime software.

3. Products affected

Systems where the COPA-DATA zenon editor is installed, are affected.

4. Versions affected

COPA-DATA zenon editor versions 8.10 and older are affected

5. 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 COPA-DATA zenon editor installed. Under specific circumstances the COPA-DATA 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 COPA-DATA 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 COPA-DATA zenon editor, the file extension .wsp6 is registered to open with the COPA-DATA zenon editor application. Removing the association for the .wsp6 file type in Windows, prevents a user from opening such a file with the 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 COPA-DATA zenon editor application only through the Windows start menu or the COPA-DATA startup tool and not make use of the possibility to open .wsp6 files directly.

6. 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](#)

[zenon version 8.00 build 60603](#)

[zenon version 8.10 build 60592](#)

7. Update

Recommendations

COPA-DATA recommends installing only the zenon runtime component on production systems and not the zenon editor.

COPA-DATA generally recommends using the COPA-DATA 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.

COPA-DATA recommends that system integrators and asset owners perform a risk assessment to establish whether the updated version of the COPA-DATA editor shall be installed.

COPA-DATA generally recommends keeping the operating system and software up to date.

COPA-DATA recommends testing the updated version of the COPA-DATA 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.

COPA-DATA 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.

8. General recommendations

COPA-DATA 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.

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

9. Acknowledgements

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



© Ing. Punzenberger COPA-DATA GmbH.

All rights reserved. This document is protected by copyright and may not be reproduced, utilized or photocopied in any form or by any means without permission in writing from Ing. Punzenberger COPA-DATA GmbH. The technical data contained herein have been provided solely for informational purposes and are not legally binding. The COPA-DATA logo, zenon, zenon Analyzer, zenon Supervisor, zenon Operator, zenon Logic and straton are registered trademarks of Ing. Punzenberger COPA-DATA GmbH. All other brands and product names may be the trademarks or registered trademarks of their representative owners. Subject to change, technical or otherwise.