

Schneider Electric Security Notification

Vijeo Designer and Vijeo Designer Basic (V1.2)

14 April 2020 (11 August 2020)

Overview

Schneider Electric is aware of a vulnerability in the Vijeo Designer and Vijeo Designer Basic Software products.

Affected Product(s)

- Vijeo Designer Basic V1.1 HotFix 15 and prior
- Vijeo Designer V6.2 SP9 and prior

Vulnerability Details

CVE ID: **CVE-2020-7490**

CVSS v3.0 Base Score 6.7 | (Medium) | CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

A CWE-426: Untrusted Search Path vulnerability exists, which could cause arbitrary code execution on the system running Vijeo Basic when a malicious DLL library is loaded by the product.

Remediation

This vulnerability is fixed in Vijeo Designer Basic version V1.1 HotFix 16. Please contact your [Schneider Electric Customer Support](#) to get Vijeo Designer Basic version V1.1 HotFix 16 software.

This vulnerability is fixed in version Vijeo Designer V6.2 SP10 released in July 2020:

- For customers using Vijeo Designer version V6.1 or earlier, please contact your [Schneider Electric Customer Support](#) to obtain the Vijeo Designer V6.2 SP10.
- For customers using a version of Vijeo Designer V6.2 or greater, Vijeo Designer V6.2 SP10 will be automatically available in Schneider Electric Software Update (SESU) software.

The following workarounds and mitigations can be applied to Vijeo Designer Basic and Vijeo Designer by customers to reduce the risk:

Schneider Electric Security Notification

- Harden the Engineering Workstation - follow workstation, network, and site hardening guidelines in the Cybersecurity Best Practices guide available for download [here](#).

Product Information

Vijeo Designer™ and Vijeo Designer™ Basic HMI software handles design from the smallest applications for 3.8” terminals to the most demanding HMI applications of 15” industrial PCs. Its open architecture adapts to all Harmony and Magelis XBT GT platforms, as well as to Harmony Smart & Compact iPCs. In addition, Vijeo Designer™ Basic is applicable to GXU platform.

Product Category - All Categories

Learn more about Schneider Electric’s product categories here: www.schneider-electric.us/en/all-products.

How to determine if you are affected

Customers using Vijeo Designer Basic V1.1 HotFix 15 and prior.

Customers using Vijeo Designer V6.2 SP9 and prior.

Note: The General tab contains the Vijeo Designer logo, name of the software, version number, and copyright information.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls to prevent unauthorized personnel from accessing your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the target network.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have been connected to any network other than the intended network to connect to the intended networks without proper sanitation.
- Minimize network exposure to all control devices and systems, and ensure that they are not accessible from the Internet.
- 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.

Schneider Electric Security Notification

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2020-7490	Yongjun Liu (nsfocus)

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

<https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp>

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability**. We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

Schneider Electric Security Notification

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 <i>14 April 2020</i>	Original Release
Version 1.1 <i>30 April 2020</i>	Corrected affected version of Vijeo Designer to V6.2 SP9 and prior (page 1)
Version 1.2 <i>11 August 2020</i>	Updated fix availability for Vijeo Designer V6.2 SP10 (page 1)