Life Is On Schneider Electric

Schneider Electric Security Notification

Vijeo Designer and Vijeo Designer Basic Software (V1.1)

12 May 2020 (11 August 2020)

Overview

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

Affected Product(s)

- Vijeo Designer Basic V1.1 HotFix 16 and prior
- Vijeo Designer V6.2 SP9 and prior

Vulnerability Details

CVE ID: **CVE-2020-7501**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

A CWE-798: Use of Hard-coded Credentials vulnerability exists which could cause unauthorized read and write when downloading and uploading project or firmware into Vijeo Designer Basic and Vijeo Designer.

Remediation

This vulnerability is fixed in version Vijeo Designer Basic V1.1 HotFix 17. Please contact your Schneider Electric Customer Support to obtain the HotFix.

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:

- Enable “Download security” to override its hardcoded password and refer to “4.8.2.2 Protecting Targets from Unauthorized Project Downloads” in online help.
- Setup network segmentation and implement a firewall to block all unauthorized access to port TCP/6001 (Not standard FTP port).

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 Magelis XBT GT platforms, as well as to Magelis Smart & Compact iPCs.

Product Category - Industrial Automation Control

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 16 and prior.

Customers using Vijeo Designer V6.2 SP9 and prior.

Note: 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.

Acknowledgements

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

CVE	Researcher(s) Name
CVE-2020-7501	Jie Chen (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.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

About Schneider Electric

Schneider Electric Security Notification

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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.

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

www.se.com

Revision Control:

Version 1.0 *12 May 2020*	Original Release
Version 1.1 *14 August 2020*	Updated fix availability for Vijeo Designer

Product Security Office

Digitally signed by Product Security Office
Date: 2020.08.08 17:20:06 -04'00'