Schneider Electric Security Notification

Vijeo Designer

10 September 2024

Overview

Schneider Electric is aware of a vulnerability in its Vijeo Designer product.

The Vijeo Designer product is HMI Configuration Software compatible with Harmony and Magelis HMI. Vijeo Designer software offers functions such as multimedia capabilities and remote access for more efficiency.

Failure to apply the remediations provided below may risk privilege escalation, which could result in unauthorized access to workstation resources.

Affected Products and Versions

Product	Version
Vijeo Designer	Versions prior to V6.3 SP1
Vijeo Designer embedded in EcoStruxure™ Machine Expert	All versions

Vulnerability Details

CVE ID: **CVE-2024-8306**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE-269: Improper Privilege Management vulnerability exists that could cause unauthorized access, loss of confidentiality, integrity and availability of the workstation when non-admin authenticated user tries to perform privilege escalation by tampering with the binaries.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
Vijeo Designer *Versions prior to V6.3 SP1*	Version V6.3 SP1 of Vijeo Designer includes a fix for this vulnerability and can be updated through the Schneider Electric Software Update (SESU) application. https://www.se.com/ww/en/product-range/1054-vijeo-designer-hmi-software/#software-and-firmware On the engineering workstation, update to v6.3 SP1 of Vijeo Designer.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Mitigations

Affected Product & Version	Mitigations
Vijeo Designer *Versions prior to V6.3 SP1*	• Limit authenticated user access to the workstation running Vijeo Designer and implement existing User Account Control practices. • Remove the write permissions for "Everyone" on the folder "C:\Program Files (x86)\Schneider Electric\Vijeo-Designer 6.3\Vijeo-Runtime" • Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices guide available for download here.
Vijeo Designer embedded in EcoStruxure™ Machine Expert *All versions*	Schneider Electric is establishing a remediation plan for all future versions of Vijeo Designer embedded in EcoStruxure™ Machine Expert that will include a fix for this vulnerability. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit:

	• Limit authenticated user access to the workstation running Vijeo Designer and implement existing User Account Control practices. • Remove the write permissions for “Everyone” on the folder “C:\Program Files (x86)\Schneider Electric\Vijeo-Designer 6.3\Vijeo-Runtime” • Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices guide available for download here.

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric’s security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

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 so no unauthorized personnel can access 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 network intended for that device.
- 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 mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system 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.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Schneider Electric Security Notification

Acknowledgements

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

CVE	Researcher
CVE-2024-8306	Charit Misra, Applied Risk (DNV Cyber)

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

About Schneider Electric

Schneider's purpose is to **create Impact** by empowering all **to make the most of our energy and resources**, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be the trusted partner in **Sustainability and Efficiency.**

Schneider Electric Security Notification

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers.**

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Revision Control:

Version 1.0.0 *10 September 2024*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.09.09 12:19:55 -04'00'