Schneider Electric Security Notification

SCADAPack Workbench

28 March 2022 (11 April 2023)

Overview

Schneider Electric is aware of a vulnerability in its SCADAPack Workbench product.

SCADAPack Workbench is a programming and configuration tool for SCADAPack 300E RTUs and SCADAPack 500E RTUs.

Failure to apply the mitigations provided below may risk information disclosure, which could result from exfiltration of data from local files to a remote system controlled by an attacker.

April 2023 Update: A remediation for the SCADAPack Workbench is available for download (page 1).

Affected Product and Versions

Product	Version
SCADAPack Workbench	Version 6.6.8a and prior

Vulnerability Details

CVE ID: **CVE-2022-0221**

CVSS v3.1 Base Score 5.5 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

A *CWE-611: Improper Restriction of XML External Entity Reference* vulnerability exists that could result in information disclosure when opening a malicious solution file provided by an attacker with SCADAPack Workbench. This could be exploited to pass data from local files to a remote system controlled by an attacker.

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
SCADAPack Workbench *Version 6.6.8a and prior*	Version 6.6.10 of SCADAPack Workbench includes a fix for this vulnerability and is available for download here: https://shop.exchange.se.com/en-US/apps/62860/scadapack-workbench-and-utilities Please follow the instructions on the download page for installation.

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 below.

Mitigations

Affected Product & Versions	Mitigations
SCADAPack Workbench *Version 6.6.8a and prior*	Schneider Electric is establishing a remediation plan for all future versions of SCADAPack Workbench 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: • Run SCADAPack Workbench as a User, not as an Administrator, to minimize the impact of malicious code on the infected system. • Do not open untrusted files with SCADAPack Workbench. • Provide training and awareness programs to educate users on the warning signs of a phishing or social engineering attack. • Employ Data Loss Prevention tools to help mitigate risk. • Restrict communication from workstations running SCADAPack Workbench to external systems. • Ensure that the least-privilege user principle is followed, and user/service account access to shared resources (such as a database) is only granted with a minimum number of rights as needed. 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.

Acknowledgements

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

CVE	Researcher
CVE-2022-0221	kimiya working with Trend Micro Zero Day Initiative

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

Schneider Electric Security Notification

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.

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 *28 March 2022*	Original Release
Version 2.0 *11 April 2023*	Remediation for the SCADAPack Workbench is available for download (page 1).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.04.10 12:30:16 -04'00'