

Schneider Electric Security Notification

EcoStruxure Power Build - Rapsody

12 January 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure Power Build - Rapsody product.

The [EcoStruxure Power Build - Rapsody](#) product is a LV switchboard configuration and quotation software to support users in the configuration and quotation process for Prisma switchboard projects in the non-critical building segment.

Failure to apply the mitigations provided below may allow remote code execution which could result in serious interruption of business operations and exfiltration of credentials and other business sensitive data.

Affected Product and Version

EcoStruxure Power Build - Rapsody software V2.1.13 and prior.

Vulnerability Details

CVE ID: **CVE-2021-22697**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists that could allow a use-after-free condition which could result in remote code execution when a malicious SSD file is uploaded and improperly parsed.

CVE ID: **CVE-2021-22698**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists that could allow a stack-based buffer overflow to occur which could result in remote code execution when a malicious SSD file is uploaded and improperly parsed.

Remediation

Schneider Electric has established a remediation plan for all future versions of EcoStruxure Power Build - Rapsody that will include a fix for these vulnerabilities. We will update this document as remediations become available in the first half of 2021. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit:

Schneider Electric Security Notification

- Apply the principle of least privilege to limit access to the computer running the Rapsody software to only those personnel that require access to it.
- Install application whitelisting software on the computer to block the execution of malicious code.
- Install anti-virus on the computer and keep it up to date.

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 for the devices that it is intended for.
- 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-2021-22697, CVE-2021-22698	rgod working Trend Micro's 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. 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 NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. 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>12 January 2021</i>	Original Release
--	------------------