# Schneider Electric Security Notification

## EcoStruxure Power Build - Rapsody

**12 January 2021 (14 June 2022)**

## 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.

June 2022 Update: Remediation added on page 2.

## Affected Product and Version

| Product | Version |
|---|---|
| EcoStruxure Power Build: Rapsody Software | Versions prior to Version 2.1.13 |

## 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

| Affected Product & Version | Remediation |
|---|---|
| **EcoStruxure Power Build: Rapsody Software**<br><br>*Versions prior to Version 2.1.13* | These vulnerabilities have been fixed in V2.1.13. Links to the fix versions in supported languages can be found below:<br><br>https://www.se.com/us/en/faqs/FA379051/ |

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:

- 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 allow list software on the computer to block the execution of malicious code.
- Install anti-virus on the computer and keep it up to date.

## 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.

# Schneider Electric Security Notification

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 these vulnerabilities:

| 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: 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 empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

# Schneider Electric Security Notification

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

| | |
|---|---|
| **Version 1.0**<br>*12 January 2021* | Original Release |
| **Version 2.0**<br>*14 June 2022* | These vulnerabilities have been fixed in V2.1.3 |

Product Security Office

Digitally signed by Product Security Office
Date: 2022.06.13 11:02:04 -04'00'