Schneider Electric Security Notification

EcoStruxure Power Commission

14 June 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure Power Commission software.

EcoStruxure Power Commission is a comprehensive software that provides strong function for setup, test and commission for low voltage power distribution switchboard.

Failure to apply the remediations provided below may risk remote code execution and Information Disclosure, which could result in loss of data integrity and confidentiality.

Affected Product and Version

Product	Versions
EcoStruxure Power Commission	Versions prior to V2.22

Vulnerability Details

CVE ID: **CVE-2022-0223**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could allow an attacker to create or overwrite critical files that are used to execute code, such as programs or libraries and cause unauthenticated code execution.

CVE ID: **CVE-2022-22731**
CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists in a function that could allow an attacker to create or overwrite critical files that are used to execute code, such as programs or libraries and cause path traversal attacks.

CVE ID: **CVE-2022-22732**

CVSS v3.1 Base Score 3.9 | Low | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N

A *CWE-668: Exposure of Resource to Wrong Sphere* vulnerability exists that could cause all remote domains to access the resources (data) supplied by the server when an attacker sends a fetch request from third-party site or malicious site.

Schneider Electric Security Notification

Remediation

Affected Product & Version	Remediation
EcoStruxure Power Commission *Versions prior to 2.22*	V2.22 and later of EcoStruxure Power Commission includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/62980-ecostruxure-power-commission/#software-and-firmware

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

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

- Configure firewall to restrict network access to authorized IP addresses as applicable.
- Use low privileged user account for running EPC. Do not run EPC with administrator privilege.
- Keep Operating System and Chrome browser up to date.
- Recommend not to use any web browser while using EPC.
- Do not open unknown or malicious websites in browser while using EPC.
- Do not click on unknown links or open attachments from unknown source.
- Train the users - Provide cybersecurity training to all your employees to help keep your organization secure. Explain phishing emails, infected attachments, malicious websites, and other methods that attack them directly.

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.
- 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 researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers
CVE-2022-0223, CVE-2022-22731, CVE-2022-22732	Noam Moshe and Amir Preminger (Claroty Research)

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

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

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.

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 *14 June 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.06.13 16:05:10 -04'00'