Schneider Electric Security Notification

PowerLogic EGX100 and PowerLogicEGX300

8 June 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in its PowerLogic EGX100 and EGX300 products.

The PowerLogic EGX100 and EGX300 are communication gateway devices.

Failure to apply the mitigations provided below may risk denial of service or remote code execution, which could result in loss of device functionality.

Affected Products and Versions

CVE	Product	Version
CVE-2021-22763	EGX100	All Versions
CVE-2021-22764, CVE-2021-22765, CVE-2021-22766, CVE-2021-22767, CVE-2021-22768	EGX100	Versions 3.0.0 and newer
CVE-2021-22763, CVE-2021-22764, CVE-2021-22765, CVE-2021-22766, CVE-2021-22767, CVE-2021-22768	EGX300	All Versions

Vulnerability Details

CVE ID: **CVE-2021-22763**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-640: Weak Password Recovery Mechanism for Forgotten Password* vulnerability exists that could allow an attacker administrator level access to a device.

CVE ID: **CVE-2021-22764**

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

A *CWE-287: Improper Authentication* vulnerability exists that could cause loss of connectivity to the device via Modbus TCP protocol when an attacker sends a specially crafted HTTP request.

CVE ID: **CVE-2021-22765**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-20: Improper Input Validation* vulnerability exists that could cause denial of service or remote code execution via a specially crafted HTTP packet.

CVE ID: **CVE-2021-22766**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-20: Improper Input Validation* vulnerability exists that could cause denial of service via a specially crafted HTTP packet.

CVE ID: **CVE-2021-22767**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-20: Improper Input Validation* vulnerability exists that could cause denial of service or remote code execution via a specially crafted HTTP packet.

CVE ID: **CVE-2021-22768**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-20: Improper Input Validation* vulnerability exists that could cause denial of service or remote code execution via a specially crafted HTTP packet.

Mitigations

PowerLogic EGX100 and EGX300 Products have reached end of service and are no longer supported. Customers should consider blocking HTTP access to the device at the firewall level once commissioning is complete to reduce the risk of exposure. Additionally, Customers should ensure the General security Recommendations listed below are in place.

Customers should also consider replacing the device with a supported product to resolve this issue. Please contact your local Schneider Electric sales representative for upgrade options.

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.

Acknowledgements

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

CVE	Researcher
CVE-2021-22763 CVE-2021-22764 CVE-2021-22765 CVE-2021-22766 CVE-2021-22767 CVE-2021-22768	Jacob Baines (Dragos)

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

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.

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 *8 June 2021*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2021.06.06 19:50:54 -04'00'