Schneider Electric Security Notification

EcoStruxure Building Operation (EBO)

10 November 2020

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure Building Operation (EBO) product offerings. More information on the product line can be found at the following link:

https://www.se.com/ww/en/product-range-presentation/62111-ecostruxure%E2%84%A2-building-operation/?parent-subcategory-id=1210&filter=business-2-building-automation-and-control#tabs-top

Failure to apply the mitigations/remediations provided below may risk various types of attacks and cause various types of impact (see information below for each vulnerability).

Affected Products and Versions

EcoStruxure Building Operation product offerings listed below

Affected Product & Version	CVE
WebReports V1.9 - V3.1	CVE-2020-7569 CVE-2020-7570 CVE-2020-7571 CVE-2020-7572 CVE-2020-7573
WebStation V2.0 - V3.1	CVE-2020-28210
Enterprise Server installer V1.9 - V3.1	CVE-2020-28209
Enterprise Central installer V2.0 - V3.1	

Vulnerability Details

CVE ID: **CVE-2020-7569**

CVSS v3.0 Base Score 4.6 | Medium | CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L

A CWE-434 Unrestricted Upload of File with Dangerous Type vulnerability exists that could cause an authenticated remote user being able to upload arbitrary files due to incorrect verification of user supplied files and achieve remote code execution.

CVE ID: **CVE-2020-7570**

CVSS v3.0 Base Score 6.4 | Medium | CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:L

A CWE-79 Improper Neutralization of Input During Web Page Generation (Cross-site Scripting Stored) vulnerability exists that could cause an authenticated remote user being able to inject arbitrary web script or HTML due to incorrect sanitization of user-supplied data and achieve a Cross-Site Scripting stored attack against other WebReport users.

CVE ID: **CVE-2020-7571**

CVSS v3.0 Base Score 6.1 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

A CWE-79 Multiple Improper Neutralization of Input During Web Page Generation (Cross-site Scripting Reflected) vulnerability exists that could cause a remote attacker to inject arbitrary web script or HTML due to incorrect sanitization of user supplied data and achieve a Cross-Site Scripting reflected attack against other WebReport users.

CVE ID: **CVE-2020-7572**

CVSS v3.0 Base Score 6.7 | Medium | CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:H

A CWE-611 Improper Restriction of XML External Entity Reference vulnerability exists that could cause an authenticated remote user being able to inject arbitrary XML code and obtain disclosure of confidential data, denial of service, server side request forgery due to improper configuration of the XML parser.

CVE ID: **CVE-2020-7573**

CVSS v3.0 Base Score 5.0 | Medium | CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L

A CWE-284 Improper Access Control vulnerability exists that could cause a remote attacker being able to access a restricted web resources due to improper access control.

CVE ID: **CVE-2020-28209**

CVSS v3.0 Base Score 2.0 | Low | CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N

A CWE-428 Windows Unquoted Search Path vulnerability exists that could cause any local Windows user who has write permission on at least one of the subfolders of the Connect Agent service binary path, being able to gain the privilege of the user who started the service. By default, the Enterprise Server and Enterprise Central is always installed at a location requiring Administrator privileges so the vulnerability is only valid if the application has been installed on a non-secure location.

CVE ID: **CVE-2020-28210**

CVSS v3.0 Base Score 4.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

A CWE-79 Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) vulnerability exists that could cause an attacker to inject HTML and JavaScript code into the user's browser.

Remediation

Version 3.2 of EBO is not impacted by any of the vulnerabilities. It is highly recommended to upgrade to this version. For assistance in upgrading, contact Schneider Electric's Customer Care Center or your Schneider Electric representative.

For versions prior to 3.2, fixes are now available in the form of a hotfix patch for the following versions and products:

Affected Product & Version	Remediation
WebReports V1.9 - V3.1	Step 1: Locate the version you need to patch on the Exchange Community by accessing community.exchange.se.com and searching for 'EBO Hotfix List' or alternatively, browse to the following URL: https://community.exchange.se.com/t5/EBO-Hotfix-List/bg-p/sbo-hotfix-list Step 2: Follow the instructions in the readme file
WebStation V2.0 - V3.1	Step 1: Locate the version you need to patch on the Exchange Community by accessing community.exchange.se.com and searching for 'EBO Hotfix List' or alternatively, browse to the following URL: https://community.exchange.se.com/t5/EBO-Hotfix-List/bg-p/sbo-hotfix-list Step 2: Follow the instructions in the readme file. Note: WebStation is not an installer of its own but is part of the EBO server (SmartX, ES or EC)
Enterprise Server installer V1.9 - V3.1	Step 1: Locate the version you need to patch on the Exchange Community by accessing community.exchange.se.com and searching for 'EBO Hotfix List' or alternatively, browse to the following URL: https://community.exchange.se.com/t5/EBO-Hotfix-List/bg-p/sbo-hotfix-list Step 2: Follow the instructions in the readme file

Enterprise Central installer V2.0 - V3.1	Step 1: Locate the version you need to patch on the Exchange Community by accessing community.exchange.se.com and searching for ‘EBO Hotfix List’ or alternatively, browse to the following URL: https://community.exchange.se.com/t5/EBO-Hotfix-List/bg-p/sbo-hotfix-list Step 2: Follow the instructions in the readme file

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 remediations provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- Do not expose any EBO Server to an untrusted network.
- Locate the EBO system behind firewalls on a segregated network. Limiting external access to only those machines and specific network ports that are necessary.
- Test and deploy Application Whitelisting on Server Machines.

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 researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2020-28210	Luis Vázquez, Francisco Palma, and Diego León of Zerolynx in coordination with INCIBE
CVE-2020-7569, CVE-2020-7570, CVE-2020-7571, CVE-2020-7572, CVE-2020-7573, CVE-2020-28209	Alessandro Bosco, Luca Di Giuseppe, Alessandro Sabetta, Massimiliano Brolli of TIM Security Red Team Research (TIM S.p.A.)

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, please 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.

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 *10 November 2020*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2020.11.08 20:51:26 -05'00'