## StruxureWare Data Center Expert

**14 February 2023**

## Overview

Schneider Electric is aware of multiple vulnerabilities in its StruxureWare Data Center Expert product.

The StruxureWare Data Center Expert product is a scalable monitoring software that collects, organizes, and distributes critical device information providing a comprehensive view of equipment.

Failure to apply the remediations provided below may risk remote access and/or Local Privilege Escalation, which could result in loss of control and loss of availability of the appliance.

## Affected Products and Versions

| Product | Version |
|---|---|
| StruxureWare Data Center Expert | V7.9.2 and earlier |

## Vulnerability Details

CVE ID: **CVE-2023-25547**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-863: Incorrect Authorization* vulnerability exists that could allow remote code execution on upload and install packages when a hacker is using a low privileged user account.

CVE ID: **CVE-2023-25548**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-863: Incorrect Authorization* vulnerability exists that could allow access to device credentials on specific DCE endpoints not being properly secured when a hacker is using a low privileged user.

CVE ID: **CVE-2023-25552**

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

A *CWE-862: Missing Authorization* vulnerability exists that could allow viewing of unauthorized content, changes or deleting of content, or performing unauthorized functions when tampering the Device File Transfer settings on DCE endpoints.

CVE ID: **CVE-2023-25554**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A *CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')* vulnerability exists that allows a local privilege escalation on the appliance when a maliciously crafted Operating System command is entered on the device.

CVE ID: **CVE-2023-25549**

CVSS v3.1 Base Score 7.2 | High | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-94: Improper Control of Generation of Code ('Code Injection')* vulnerability exists that allows for remote code execution when using a parameter of the DCE network settings endpoint.

CVE ID: **CVE-2023-25550**

CVSS v3.1 Base Score 7.2 | High | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

A *CWE-94: Improper Control of Generation of Code ('Code Injection')* vulnerability exists that allows remote code execution via the “hostname” parameter when maliciously crafted hostname syntax is entered.

CVE ID: **CVE-2023-25551**

CVSS v3.1 Base Score 6.1 | Medium | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists on a DCE file upload endpoint when tampering with parameters over HTTP.

CVE ID: **CVE-2023-25553**

CVSS v3.1 Base Score 6.1 | Medium | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists on a DCE endpoint through the logging capabilities of the webserver.

CVE ID: **CVE-2023-25555**

CVSS v3.1 Base Score 5.6 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

A *CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')* vulnerability exists that could allow a user that knows the credentials to execute unprivileged shell commands on the appliance over SSH.

## Remediation

| Affected Product & Version | Remediation |
|---|---|
| **StruxureWare Data Center Expert**<br>*V7.9.2 and earlier* | Version 7.9.3 of StruxureWare Data Center Expert includes fixes for these vulnerabilities and is available on request from Schneider Electric's Customer Care Center. |

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 general security recommendations to reduce the risk of exploit:

Harden the DCE instance according to the cybersecurity best practices documented in the Data Center Expert Security Handbook

## 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.

## 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

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.

Revision Control:

| | |
|---|---|
| **Version 1.0**<br>*14 February 2023* | Original Release |

Product Security Office Digitally signed by Product Security Office
Date: 2023.02.13 13:14:14 -05'00'