

# Schneider Electric Security Notification

## Data Center Expert

8 October 2024

### Overview

Schneider Electric is aware of a vulnerability in its Data Center Expert product.

The [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 fix provided below may risk information disclosure, which could result in access to private data.

### Affected Products and Versions

Product	Version
Data Center Expert	Versions 8.1.1.3 and prior

### Vulnerability Details

CVE ID: **CVE-2024-8531**

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

*CWE-347: Improper Verification of Cryptographic Signature* vulnerability exists that could compromise the Data Center Expert software when an upgrade bundle is manipulated to include arbitrary bash scripts that are executed as root.

CVE ID: **CVE-2024-8530**

CVSS v3.1 Base Score 5.9 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

*CWE-306: Missing Authentication for Critical Function* vulnerability exists that could cause exposure of private data when an already generated “logcaptures” archive is accessed directly by HTTPS.

*Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 ([CVSS v3.1](#)) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer’s environment.*

## Schneider Electric Security Notification

### Remediation

Affected Product & Version	Remediation
EcoStruxure™ IT Data Center Expert Versions 8.1.1.3 and earlier  (Formerly known as StruxureWare Data Center Expert)	Version 8.2 of EcoStruxure™ IT Data Center Expert includes fixes for these vulnerabilities and is available upon request from Schneider Electric’s <a href="#">Customer Care Center</a> .

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:

### Mitigations

- Ensure that the principals of least privilege are being followed so that only those with need have account access and that the level of their respective account authorization aligns with their role, including Privileged Accounts as described in the [Data Center Expert Security Handbook](#).
- Verify SHA1 checksums of upgrade bundles prior to executing upgrades as described in the Upgrades section of the [Data Center Expert Security Handbook](#).
- Delete any existing “logcapture” archives present on the system and do not create any new “logcapture” archives. Existing archives can be deleted from the [https://server\\_ip/capturelogs](https://server_ip/capturelogs) web page after authenticating.

### 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 intended for that device.

## Schneider Electric Security Notification

- 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-2024-8530	Anonymous working with Trend Micro 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>

#### 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,

## Schneider Electric Security Notification

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 **create Impact** by empowering 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 the trusted partner in **Sustainability and Efficiency**.

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers**.

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

[www.se.com](http://www.se.com)

Revision Control:

<p><b>Version 1.0.0</b> 08 October 2024</p>	<p>Original Release</p>
---	-------------------------