

Schneider Electric Security Notification

EcoStruxure™ IT Data Center Expert

8 July 2025

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ IT Data Center Expert (DCE) product.

The [EcoStruxure™ IT 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 remediation provided below may risk information disclosure, and remote compromise of the offer which could result in disruption of operations and access to system data.

Affected Products and Versions

Product	Version
EcoStruxure™ IT Data Center Expert	Versions v8.3 and prior

Vulnerability Details

CVE ID: **CVE-2025-50121**

CVSS v3.1 Base Score 10 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Base Score 9.5 | Critical | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:L/SA:H

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability exists that could cause unauthenticated remote code execution when a malicious folder is created over the web interface HTTP when enabled. HTTP is disabled by default.

CVE ID: **CVE-2025-50122**

CVSS v3.1 Base Score 8.3 | High | CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Base Score 8.9 | High | CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:L/SA:H

CWE-331: Insufficient Entropy vulnerability exists that could cause root password discovery when the password generation algorithm is reverse engineered with access to installation or upgrade artifacts.

Schneider Electric Security Notification

CVE ID: **CVE-2025-50123**

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

CVSS v4.0 Base Score 7.2 | High | CVSS:4.0/AV:P/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:L/SA:H

CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that could cause remote command execution by a privileged account when the server is accessed via a console and through exploitation of the hostname input.

CVE ID: **CVE-2025-50125**

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

CVSS v4.0 Base Score 6.3 | Medium | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:N/SA:N

CWE-918: Server-Side Request Forgery (SSRF) vulnerability exists that could cause unauthenticated remote code execution when the server is accessed via the network with knowledge of hidden URLs and manipulation of host request header.

CVE ID: **CVE-2025-50124**

CVSS v3.1 Base Score 6.9 | Medium | CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Base Score 7.2 | High | CVSS:4.0/AV:P/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:L/SA:H

CWE-269: Improper Privilege Management vulnerability exists that could cause privilege escalation when the server is accessed by a privileged account via a console and through exploitation of a setup script.

CVE ID: **CVE-2025-6438**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N

CVSS v4.0 Base Score 5.9 | Medium | CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:N/VA:N/SC:L/SI:N/SA:N

CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause manipulation of SOAP API calls and XML external entities injection resulting in unauthorized file access when the server is accessed via the network using an application account.

The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 (CVSS v4.0). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated 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 <i>Versions 8.3 and prior</i> (Formerly known as StruxureWare Data Center Expert)	Version 9.0 of EcoStruxure™ IT Data Center Expert includes fixes for these vulnerabilities and is available upon request from Schneider Electric's Customer Care Center .

Customers should use appropriate methodologies when applying these upgrades to their systems. We strongly recommend the use of back-ups and evaluating the impact of these upgrades in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's [Customer Care Center](#) if you need assistance.

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

- Harden the DCE instance according to the cybersecurity best practices documented in the [EcoStruxure™ IT 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 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.

Schneider Electric Security Notification

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2025-50121 CVE-2025-50122 CVE-2025-50123 CVE-2025-50124 CVE-2025-50125 CVE-2025-6438	Jaggar Henry, KoreLogic, Inc. Jim Becher, KoreLogic, Inc.

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 **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**.

Schneider Electric Security Notification

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

Revision Control:

Version 1.0.0 08 July 2025	Original Release
--------------------------------------	------------------