مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates-EcoStruxure IT Data Center Expert (DCE)

Tracking #:432317464

Date:11-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Schneider Electric has disclosed multiple critical and high-severity vulnerabilities in its EcoStruxure IT Data Center Expert (DCE) platform, which is widely used for centralized monitoring of data center infrastructure.

TECHNICAL DETAILS:

Schneider Electric has disclosed multiple critical and high-severity vulnerabilities in its EcoStruxure IT Data Center Expert (DCE) platform, which is widely used for centralized monitoring of data center infrastructure.

If left unpatched, these vulnerabilities could allow unauthenticated remote code execution, privilege escalation, sensitive data access, and server-side request forgery (SSRF). Exploitation may lead to complete system compromise, disruption of operations, or unauthorized access to critical infrastructure data.

Immediate remediation is essential to reduce the risk of exploitation, especially in internet-facing deployments or environments with weak access controls.

Vulnerability Details:

1. CVE-2025-50121 – OS Command Injection via HTTP Web Interface
   - Severity: Critical
   - CVSS v3.1: 10.0 | CVSS v4.0: 9.5
   - Allows unauthenticated remote code execution via specially crafted folder names if HTTP is enabled.
   - Attack Vector: Remote (Network)

2. CVE-2025-50122 – Weak Password Entropy
   - Severity: High
   - CVSS v3.1: 8.3 | CVSS v4.0: 8.9
   - Predictable root password due to weak entropy in generation algorithm.
   - Exploitable via access to installation/upgrade artifacts.

3. CVE-2025-50123 – Code Injection via Hostname Input
   - Severity: High
   - CVSS v3.1 & v4.0: 7.2
   - Privileged remote command execution when hostname input is manipulated through console access.

4. CVE-2025-50125 – Server-Side Request Forgery (SSRF)
   - Severity: High/Medium
   - CVSS v3.1: 7.2 | CVSS v4.0: 6.3
   - SSRF attack via manipulation of hidden URLs and Host headers.
   - Could lead to unauthenticated remote code execution.

5. CVE-2025-50124 – Improper Privilege Management
   - Severity: Medium/High
   - CVSS v3.1: 6.9 | CVSS v4.0: 7.2
   - Privilege escalation by abusing setup scripts accessible via console.

6. CVE-2025-6438 – XML External Entity (XXE) Injection
   - Severity: Medium
   - CVSS v3.1: 6.8 | CVSS v4.0: 5.9
   - SOAP/XML parsing vulnerability that may allow unauthorized file access via API calls using application credentials.

Fixed version:

- EcoStruxure IT Data Center Expert version 9.0.

RECOMMENDATIONS:

- Upgrade Immediately
  - Upgrade EcoStruxure IT Data Center Expert to fixed version.
  - Contact Schneider Electric Customer Care Center to obtain the upgrade.
- Disable HTTP Interface
  - Ensure it remains disabled or use HTTPS only.
- Restrict Console Access
  - Limit local and remote console access to authorized personnel only.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2025-189-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2025-189-01.pdf