Schneider Electric Security Notification

Data Center Expert

14 June 2022 (16 June 2022)

Overview

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

The Data Center Expert product provides an efficient way for organizations to monitor and manage their company-wide multi-vendor physical infrastructure, including power, cooling, security and environmental.

Failure to apply the remediations provided below may risk unauthorized access to a DCE instance, which could result in downtime or outage.

June 16 2022 Update: Affected versions updated to include V7.9.0, remediation guidance updated for clarity.

Affected Product and Versions

Product	Version
Data Center Expert	V7.9.0 and prior

Vulnerability Details

CVE ID: **CVE-2022-32518**

CVSS v3.1 Base Score 8.0 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

A *CWE-522*: *Insufficiently Protected Credentials* vulnerability exists that could result in unwanted access to a DCE instance when performed over a network by a malicious third-party. This CVE is unique from CVE-2022-32520.

CVE ID: **CVE-2022-32519**
CVSS v3.1 Base Score 8.0 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

A *CWE-257*: *Storing Passwords in a Recoverable* Format vulnerability exists that could result in unwanted access to a DCE instance when performed over a network by a malicious third-party.

CVE ID: **CVE-2022-32520**
CVSS v3.1 Base Score 8.0 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

A *CWE-522: Insufficiently Protected Credentials* vulnerability exists that could result in unwanted access to a DCE instance when performed over a network by a malicious third-party. This CVE is unique from CVE-2022-32518.

CVE ID: **CVE-2022-32521**
CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

Schneider Electric Security Notification

A *CWE 502*: *Deserialization of Untrusted Data* vulnerability exists that could allow code to be remotely executed on the server when unsafely deserialized data is posted to the web server.

Remediation

Affected Product & Version	Remediation
Data Center Expert *V7.9.0 and prior*	Data Center Expert V7.9.1 and newer includes fixes for these vulnerabilities. You can download the latest version on the EcoStruxure IT Entitlements Portal. If you do not have an EcoStruxure IT Entitlements account, please contact Customer Care Center. Release Notes: https://dcimsupport.ecostruxureit.com/hc/en-us/articles/4517646198941-Data-Center-Expert-7-9-1-release-notes

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:

- Leverage secure protocols wherever available (HTTPS)
- Leverage certificates signed by an external and trusted CA

Follow security hardening guidelines found in https://dcimsupport.ecostruxureit.com/hc/en-us/articles/360039289633-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.
- 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 these vulnerabilities:

CVE	Researchers
CVE-2022-32521	Tom Wyatt of Mimecast Ltd
CVE-2022-32518, CVE-2022-32519, CVE-2022-32520	Chris Schatz of CrowdStrike

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

Schneider Electric Security Notification

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.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.

www.se.com

Revision Control:

Version 1.0 *14 June 2022*	Original Release
Version 2.0 *16 June 2022*	Affected versions updated to include V7.9.0, remediation guidance updated for clarity.

Product Security Office

Digitally signed by Product Security Office
Date: 2022.06.16 13:49:56 -04'00'