Data Center Expert

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

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Expert</td>
<td>V7.9.0 and prior</td>
</tr>
</tbody>
</table>

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**
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

<table>
<thead>
<tr>
<th>Affected Product &amp; Version</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Expert V7.9.0 and prior</td>
<td>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.</td>
</tr>
</tbody>
</table>


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


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

<table>
<thead>
<tr>
<th>CVE</th>
<th>Researchers</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2022-32521</td>
<td>Tom Wyatt of Mimecast Ltd</td>
</tr>
<tr>
<td>CVE-2022-32518,</td>
<td>Chris Schatz of CrowdStrike</td>
</tr>
<tr>
<td>CVE-2022-32519,</td>
<td></td>
</tr>
<tr>
<td>CVE-2022-32520</td>
<td></td>
</tr>
</tbody>
</table>

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](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.

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:

<table>
<thead>
<tr>
<th>Version 1.0</th>
<th>Original Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 June 2022</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version 2.0</th>
<th>Original Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 June 2022</td>
<td>Affected versions updated to include V7.9.0, remediation guidance updated for clarity.</td>
</tr>
</tbody>
</table>

Product Security Office

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