8 September 2020 (9 February 2021)

Overview

Schneider Electric is aware of multiple vulnerabilities in the SCADAPack x70 Remote Connect and the SCADAPack x70 Security Administrator applications.

February 2021 update: Replaced CVE-2020-7528 with the pre-existing CVE-2020-12525 assigned to M&M Software, eliminating the duplicate entry for the same vulnerability.

Affected Products and Versions

<table>
<thead>
<tr>
<th>Affected Product &amp; Version</th>
<th>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCADAPack x70 Remote Connect</td>
<td>CVE-2020-12525, CVE-2020-7529, CVE-2020-7530, CVE-2020-7531</td>
</tr>
<tr>
<td>V3.6.3.574 and prior.</td>
<td></td>
</tr>
<tr>
<td>SCADAPack x70 Security Administrator</td>
<td>CVE-2020-7532</td>
</tr>
<tr>
<td>V1.2.0 and prior.</td>
<td></td>
</tr>
</tbody>
</table>

Vulnerability Details

CVE ID: **CVE-2020-12525**


M&M Software fdtCONTAINER Component in versions below 3.5.20304.x and between 3.6 and 3.6.20304.x which is included in SCADAPack x70 is vulnerable to deserialization of untrusted data in its project storage.

CVE ID: **CVE-2020-7529**

CVSS v3.0 Base Score 5.5 | Medium | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

A CWE-22 Improper Limitation of a Pathname to a Restricted Directory (‘Path Transversal’) vulnerability exists which allows an attacker to place content in any unprotected folder on the target system using a crafted .RCZ file.

CVE ID: **CVE-2020-7530**

CVSS v3.0 Base Score 7.1 | High | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

A CWE-285 Improper Authorization vulnerability exists which allows improper access to executable code folders.
CVE ID: **CVE-2020-7531**
A CWE-284 Improper Access Control vulnerability exists which allows an attacker to place executables in a specific folder and run code whenever RemoteConnect is executed by the user.

CVE ID: **CVE-2020-7532**
CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
A CWE-502 Deserialization of Untrusted Data vulnerability exists which could allow arbitrary code execution when an attacker builds a custom .SDB file containing a malicious serialized buffer.

**Remediation**
For SCADAPack x70 Remote Connect and SCADAPack x70 Security Administrator these vulnerabilities are fixed in SCADAPack x70 RemoteConnect V3.7.3.904 and SCADAPack x70 Security Administrator V1.6.2 respectively and are available for download in the link below, as part of the RemoteConnect V2.4.2 package:


There is no need to reboot.

The following workarounds and mitigations can be applied by customers to reduce the risk:
- Educate users to screen files from external sources and avoid files from untrusted sources before opening them in RemoteConnect or Security Administrator.

**Product Information**

**SCADAPack x70 RemoteConnect** is a single software tool for users to monitor, configure, program, and commission SCADAPack 470, 474, 570, 574, and 575 Smart RTUs (Remote Terminal Units).

**SCADAPack x70 Security Administrator** is a security tool designed to configure security for SCADAPack E controllers communicating using DNP3 and AGA12-2 standards.

**Product Category** - Industrial Automation Control

Learn more about Schneider Electric’s product categories here: https://www.se.com/us/en/all-products

**How to determine if you are affected**
If you are running SCADAPack x70 RemoteConnect V3.6.3.574 and prior or SCADAPack x70 Security Administrator V1.2.0 and prior.
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 for the devices that it is intended for.
- 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 laptops 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.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to this vulnerability:

<table>
<thead>
<tr>
<th>CVE</th>
<th>Researcher Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2020-7529,</td>
<td>Amir Preminger of Claro</td>
</tr>
<tr>
<td>CVE-2020-7530,</td>
<td>ty</td>
</tr>
<tr>
<td>CVE-2020-7531,</td>
<td></td>
</tr>
<tr>
<td>CVE-2020-7532</td>
<td></td>
</tr>
</tbody>
</table>

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, please contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp
Legal Disclaimer

THIS DOCUMENT IS 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 OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER 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. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe access to energy and digital is a basic human right. We empower all to make the most of their energy and resources, ensuring Life Is On everywhere, for everyone, at every moment.

We provide energy and automation digital solutions for efficiency and sustainability. We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an open, global, innovative community that is passionate about our 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>8 September 2020</td>
<td>Corrected fix version of RemoteConnect from V2.3.2 to V2.4.2 package (page 2)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version 1.1</th>
<th>Original Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 October 2020</td>
<td>Replaced CVE-2020-7528 with the pre-existing CVE-2020-12525 assigned to M&amp;M Software, eliminating the duplicate entry for the same vulnerability. (page 1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Version 1.2</th>
<th>Original Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 February 2021</td>
<td>Digitally signed by Product Security Office</td>
</tr>
</tbody>
</table>

Date: 2021.02.07 19:46:04 -05'00'

Digitally signed by Product Security Office