Important security notification – SCADAPack 330, SCADAPack 334, SCADAPack 350, and SCADAPack 357 Firmware

December 11, 2013

Schneider Electric® has become aware of a vulnerability involving an open VxWorks debug port as described in ICS-CERT Advisory ICSA-10-214-01

The vulnerability identified:

UDP port 17185 is open by default. This open debug port could be exploited by an attacker to facilitate a denial-of-service attack, or in some cases even fully compromise the device. There is no evidence that this vulnerability has been exploited.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Details on Products Affected

The following product firmware versions are affected:

SCADAPack 33x firmware 1.71 or earlier
SCADAPack 35x firmware 1.71 or earlier

Details on workarounds or planned fix dates for above described Vulnerability

Schneider Electric has fixed this issue in the latest released firmware versions for the SCADAPack products listed above by closing this UDP port. The version 1.72 firmware may be obtained from this link: https://cmi.sharefile.com/d/sf01ee16ecb043569. If problems are encountered with the link, please email TRSS-Support@Schneider-Electric.com and request the latest firmware loader for SCADAPack 3xx controllers, or contact your local Schneider Electric office for latest firmware version for these SCADAPack products.

If it is not possible to apply the new firmware to an existing installation at this time, then Schneider Electric has produced a recommendations document that describes firewall and network architecture settings that can be used to mitigate these vulnerabilities. That document is contained in Resolution 207869 Mitigation of vulnerabilities. Please contact your local Schneider Electric office for more information.

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System. This approach places the PLCs behind one or more firewalls to restrict access to authorized personnel and protocols only. The location of the firewalls is decided based on how large the trusted zone is required to be. Please read the following document for more detailed information:

http://download.schneider-electric.com/files?p_File_Id=305147922&p_File_Name=Cyber-Security-STN-v2-Aug-2012.pdf

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system they should be adapted by individual users as required.

Windriver Debug port : Overall CVSS Score: 9.0
(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:O/RC:C/CDP:MH/TD:H/CR:L/IR:H/AR:M)

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com