August, 2015

RESOLUTION - FA198697
(Replaces previous RES206895 V3)

Important security notification – M340, Quantum, Premium and STB Ethernet communication modules (ICS-ALERT-11-346-01)

Updated Aug 20, 2015 (to reference FTP disable feature in M340 PLC range).
This is an update to a document dated August 17, 2012 and May 7, 2013

Schneider Electric® has become aware of multiple vulnerabilities in the Ethernet modules of its M340, Quantum, Premium PLC ranges and STB I/O.

The vulnerabilities identified include:

1. Telnet port accessible by end users allowing remote attackers to view the operation of the firmware modules, cause denial of service, modify the memory of the module and execute arbitrary code
2. Windriver™ Debug port used for development accessible to end users allowing remote attackers to view the operation of the firmware modules, cause denial of service, modify the memory of the module and execute arbitrary code
3. FTP service accessible to end users allowing a user to modify the module web site, download and run custom firmware and modify http passwords
4. Multiple hardcoded credentials that enable access to the above services

Please note, all of these vulnerabilities would require network access to the target device.

These vulnerabilities were discovered during cyber security research both by an external researcher and by Schneider Electric's internal investigations. Schneider Electric has no evidence that these vulnerabilities have been exploited at customer sites.

Schneider Electric takes these vulnerabilities very seriously and has devoted resources to immediately investigate and address these issues. It is critical to consider safety, security and reliability when addressing such issues and any patches, solutions and/or mitigations released by Schneider Electric will be carefully tested to ensure they can be deployed safely and securely.

Details on effected products

The following products are affected:

Quantum

- 140NOE77101 Firmware Version 4.9 and all previous versions
- 140NOE77111 Firmware Version 5.0 and all previous versions
- 140NOE77100 Firmware Version 3.4 and all previous versions
- 140NOE77110 Firmware Version 3.3 and all previous versions
- 140CPU65150 Firmware Version 3.5 and all previous versions
- 140CPU65160 Firmware Version 3.5 and all previous versions
- 140CPU65260 Firmware Version 3.5 and all previous versions
- 140NOC77101 Firmware Version 1.01 and all previous versions

Any available Conformal Coated versions of the above part numbers

Premium

- TSXETY4103 Firmware Version 5.0 and all previous versions
- TSXETY5103 Firmware Version 5.0 and all previous versions
- TSXP571634M Firmware Version 4.9 and all previous versions
- TSXP572634M Firmware Version 4.9 and all previous versions
- TSXP573634M Firmware Version 4.9 and all previous versions
- TSXP574634M Firmware Version 3.5 and all previous versions
- TSXP575634M Firmware Version 3.5 and all previous versions
- TSXP576634M Firmware Version 3.5 and all previous versions
- TSXETC101 Firmware Version 1.01 and all previous versions

Any available Conformal Coated versions of the above part numbers

M340

- BMXNOE0100 Firmware Version 2.3 and all previous versions
- BMXNOE0110 Firmware Version 4.65 and all previous versions
- BMXP342020 Firmware Version 2.2 and all previous versions
- BMXP342030 Firmware Version 2.2 and all previous versions
- BMXNOC0401 Firmware Version 1.01 and all previous versions

The following products are **not** affected by the Telnet or Windriver debug port vulnerabilities:

- BMXP342020
- BMXP342030
- STBNIC2212
- STBNIP2212
- STBNIP2311

The following products support HTTP and FTP service enable and disable feature:

- 140NOE77101 Firmware Version 06.00
- 140NOE77111 Firmware Version: 06.00
- BMXP34xxxx controller and associated Ethernet communication modules

Recommendations

1. Telnet and Windriver Debug ports

Schneider Electric has developed fixes for the Telnet and Windriver debug port vulnerabilities for all modules. This fix removes those services from the modules. New firmware versions are available on the Schneider Electric corporate website or your local country website.

Please note, this fix WILL NOT affect the capacities/functionalities of the product or impact the performance of your installation. Telnet and Windriver Debug services are installed for use by developers only and are not intended for use by customers.

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

2. FTP Service

Schneider Electric has added a new feature that allows users to disable FTP service on modules. Please refer to the above list to check if your device is supported.

If the FTP service is required, a recommendations document has been produced by Schneider Electric that describes firewall and network architecture settings that can be used to mitigate these vulnerabilities. That document is contained in Resolution 207869. Please contact your local Schneider Electric office for more information.

3. Hardcoded Credentials

The vulnerability exposed by hardcoded credentials is mitigated considerably by removing Telnet services and limiting access to FTP services. With the addition of a new feature, users now have the capability to disable the FTP service in the device. Please refer to the above list to check if your device is supported.

Please note, some of these credentials are included by design for services like FDR to function, allowing users to replace existing devices without the need to enter any configuration information (including passwords needed to download the devices configuration from the server). In addition, some of these credentials are included by design to allow easy operation of tools such as OS Loader and Web Designer.

Schneider Electric is evaluating options to modify the use of these tools to improve security while preserving customer experience. Prior to a full resolution, the mitigation actions provided in this document will reduce the risk of exploitation of this vulnerability.

4. 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:
www2.schneider-electric.com%2Fsites%2Fcorporate%2Fen%2Fsupport%2Fcybersecurity%2Fcybersecurity.page&ei=xmrXVbcyyqd6lO2ZiA4&usg=AFQjCNGJ_c4tMFsmyz08b_MERa2R9sawcg&sig2=1g8CckOdvObk1QFaC6NHYQ

Acknowledgments

Schneider Electric wishes to thank researcher Ruben Santamarta for reporting these vulnerabilities and working with us during the disclosure process.

Support

If you are unsure whether you could be effected by this vulnerability or if you have any questions on this issue please contact your local Schneider Electric support center.

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)
Telnet port with hard coded credentials : Overall CVSS Score : 8.5
(AV:N/AC:L/Au:S/C:C/I:C/A:C/E:F/RL:O/RC:C/CDP:MH/TD:H/CR:L/IR:H/AR:M)
FTP port with hard coded credentials : Overall CVSS Score 8.4
(AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:T/RC:C/CDP:MH/TD:H/CR:L/IR:H/AR:M)
TFTP Port with hard coded credentials : Overall CVSS Score : 8.8
(AV:N/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:T/RC:C/CDP:MH/TD:H/CR:L/IR:H/AR:M)