Schneider Electric Security Notification

Embedded TCP/IP Stacks Vulnerabilities (AMNESIA:33) in Modicon TM5 modules

12 October 2021

Overview

Schneider Electric is aware of multiple embedded TCP/IP stacks vulnerabilities, known as "AMNESIA:33". The Modicon TM5 modules are affected by two of these vulnerabilities. The complete details of the AMNESIA:33 vulnerabilities can be found in the Forescout report.

Modicon TM5 are I/O configuration modules for automation solutions based on Modicon and PacDrive 3 controllers.

Failure to apply the remediations provided below may risk network attacks which could result in Denial of Service or arbitrary code execution on the modules.

Affected Products and Versions

Product	Version
TM5CSLC100FS: safety logic controller	Firmware V2.56 and prior
TM5CSLC200FS: safety logic controller	Firmware V2.56 and prior
TM5NS31: sercos III communication module	Firmware V2.78 and prior
TM5NEIP1: EtherNet/IP module	Firmware V3.10 and prior
TM5NEIP1K: EtherNet/IP FieldBus KIT	Firmware V3.10 and prior

Vulnerability Details

CVE ID: **CVE-2020-13987**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Original description: An Out-of-Bounds Read vulnerability exists in the uIP TCP/IP Stack component when calculating the checksums for IP packets in upper_layer_cheksum in net/ipv4/uip.c.

CVE ID: **CVE-2020-17438**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Original description: An issue was discovered in uIP 1.0, as used in Contiki 3.0 and other products. The code that reassembles fragmented packets fails to properly validate the total length of an incoming packet specified in its IP header, as well as the fragmentation offset value

specified in the IP header. By crafting a packet with specific values of the IP header length and the fragmentation offset, attackers can write into the .bss section of the program (past the statically allocated buffer that is used for storing the fragmented data) and cause a denial of service in uip_reass() in uip.c, or possibly execute arbitrary code on some target architectures.

Remediation

The Modicon TM5 modules below have a fix for these vulnerabilities.

Affected Product & Version	Remediation
TM5CSLC100FS *Firmware V2.56 and prior*	1. On the engineering workstation, update to EcoStruxure Machine Expert v2.0.1 or above: https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert-%28somachine%29/?selected-node-id=14435955187#/software-firmware-tab 2. Use device assistant tool provided with EcoStruxure Machine Expert and upgrade TM5CSLC100FS firmware version v2.57. A reboot of the module is needed.
TM5CSLC200FS *Firmware V2.56 and prior*	1. On the engineering workstation, update to EcoStruxure Machine Expert v2.0.1 or above: https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert-%28somachine%29/?selected-node-id=14435955187#/software-firmware-tab 2. Use device assistant tool provided with EcoStruxure Machine Expert and upgrade TM5CSLC200FS firmware version v2.57. A reboot of the module is needed.
TM5NS31 *Firmware V2.78 and prior*	1. On the engineering workstation, update to EcoStruxure Machine Expert v2.0.1 or above: https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert-%28somachine%29/?selected-node-id=14435955187#/software-firmware-tab 2. Use device assistant tool provided with EcoStruxure Machine Expert and upgrade TM5NS31 firmware version v2.79. A reboot of the module is needed.
TM5NEIP1 *Firmware V3.10 and prior*	Please contact your local Schneider Electric technical support for more information on how to upgrade firmware to version v3.12

Schneider Electric Security Notification

TM5NEIP1K *Firmware V3.10 and prior*	Please contact your local Schneider Electric technical support for more information on how to upgrade firmware to version v3.12

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:

Restrict network access to the controller connected to the TM5 module via network segmentation and network access controls

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here:

https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

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 intended for that device.
- 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.

Schneider Electric Security Notification

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

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, 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 with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control

Version 1.0 *12 October 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.10.08 23:22:08 -04'00'