Schneider Electric Security Notification

Unity Loader and OS Loader Software

9 June 2020

Overview

Schneider Electric is aware of a vulnerability in the Unity loader and OS Loader, products used to upgrade firmware on Modicon controllers.

Affected Product(s)

- Unity Loader - All versions
- OS Loader - All versions (used for legacy Modicon offers)
  OS Loader is available from UnityPro and Ecostruxure Control Expert.

Vulnerability Details

CVE ID: **CVE-2020-7498**

CVSS v3.0 Base Score 10 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A CWE-798: Use of Hard-coded Credentials vulnerability exists in the Unity Loaders and OS Loader products. The fixed credentials are used to simplify file transfer. Today the use of fixed credentials is considered a vulnerability, which could cause unauthorized access to the file transfer service provided by the Modicon PLCs. This could result in various unintended results.

Remediation

Hardcoded credentials are kept for compatibility with legacy products. To mitigate the risks linked to this vulnerability on Unity Loader and OS Loader (for legacy offers Premium and Quantum), users should immediately apply the following instructions:

General Mitigations:

- Set up network segmentation and implement a firewall to block all unauthorized access to port TCP/21.

Modicon M580 CPU:

- As a proactive control, consider keeping deactivated FTP services on devices by default and while not in use. FTP is needed only during maintenance for firmware upload. To deactivate FTP, use “Security TAB” section of “Modicon M580 Hardware Reference Manual”:
  https://www.se.com/ww/en/download/document/EIO0000001578/

- Change default FTP credential on M580 Modicon PLCs: In Control Expert modify FTP password according to section “Firmware Protection” in “EcoStruxure™ Control Expert Operating Modes”:

  https://www.se.com/ww/en/download/document/33003101K01000/

- Enforce Access Control Lists on Modicon PLC: set up secure communication according to the following guideline “Modicon Controllers Platform Cyber Security Reference Manual,” in chapter “Set up secured communications”:

  https://www.se.com/ww/en/download/document/EIO0000001999/

Modicon M340 CPU:

- As a proactive control, consider keeping deactivated FTP services on devices by default and while not in use. FTP is needed only during maintenance for firmware upload. This is documented in the EcoStruxure Control Expert Help via EcoStruxure Control Expert > Help (top menu).

  To activate/deactivate FTP Service go to “Modicon M340 Platform > Modicon M340 Communication > Ethernet Communications for Modicon M340 > Ethernet Configuration with Control Expert > Software Configuration Parameters > Security”.

- Enforce Access Control Lists on Modicon PLC following the following guideline “Modicon M340 for Ethernet - Communication Modules and Processors, User Manual”: Refer to “Security section” and “Messaging Configuration Parameters section”:

  https://www.se.com/ww/en/download/document/31007131K01000/

Modicon Momentum:

- Enforce Access Control Lists on Modicon PLC following the guideline “Modicon M340 Deactivate FTP server – attached to BOOTP/DHCP service”, detailed in section “Configuring the Momentum 170ENT11001 IP Parameters” of user guide:

  https://www.se.com/ww/en/download/document/31004109K01000/

Legacy offers: Modicon Quantum / Modicon Premium

Schneider Electric's Modicon Quantum / Premium controllers have reached their end of life and are no longer commercially available. They have been replaced by the Modicon M580 ePAC controller, our current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC.

Please contact your local Schneider Electric technical support for more information.

- **Modicon Quantum**:
  Configure the Access Control List feature as mentioned in "Quantum using EcoStruxure™ Control Expert - TCP/IP Configuration, User Manual" in chapter "Software Settings for Ethernet Communication / Messaging / Quantum NOE Ethernet Messaging Configuration":
  https://www.se.com/ww/en/download/document/33002467K01000/

- **Modicon Premium:**
  Configure the Access Control List following the recommendations of the user manual "Premium and Atrium using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual" in chapters "Connection configuration parameters / TCP/IP Services Configuration Parameters / Connection Configuration Parameters":
  https://www.se.com/ww/en/download/document/35006192K01000/

Product Information

Unity Loader software is a utility to exchange data with the Modicon M340, Modicon M580, and Modicon Momentum.

OS Loader software is a utility to exchange data with Modicon Quantum / Premium processors, Quantum/Premium processors with Ethernet ports, Quantum processors with Hot Standby coprocessors, Quantum/Premium Ethernet modules (140NOE771*, 140NOC78*, 140CRP312 00, TSXETY*), Quantum S908 RIO communication modules (140CRP93*, 140CRA93*).

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

- All users of Unity Loader
- All users of OS Loader feature provided with Unity Pro and Ecostruxure Control Expert

General Security Recommendations

We strongly recommend 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(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2020-7498	Yang Dong (DingXiang Dongjian Security Lab)

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 and Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

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:

Version 1 *9 June 2020*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2020.06.07 14:19:20 -04'00'