America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Schneider Electric Modicon Modbus Protocol

Last Revised: April 11, 2017 **Alert Code:** ICSA-17-101-01

CVSS v3 10.0

ATTENTION: Remotely exploitable/low skill level to exploit.

Vendor: Schneider Electric

Equipment: Modicon Modbus Protocol

Vulnerabilities: Authentication Bypass by Capture-Replay, Violation of Secure Design Principles

AFFECTED PRODUCTS

The following versions of Modicon Modbus protocol, which can be used with the Modicon family of programmable logic controllers (PLCs), are affected:

- Modicon Modbus protocol, all versions.

IMPACT

Successful exploitation of these vulnerabilities may allow an unauthorized remote attacker to capture and replay sensitive commands to PLCs on a network using the Modicon Modbus protocol.

MITIGATION

Schneider Electric has reported that they have introduced compensating controls to limit the exploitability of the identified vulnerabilities in many of the PLCs in the Modicon family; however, Schneider Electric recommends that users apply security measures to improve resiliency.

Schneider Electric's Momentum M1E controllers (all versions of model 171CBU98090 and all versions of model 171CBU98091) do not have built-in compensating controls to limit the exploitability of the identified vulnerabilities and Schneider Electric instructs users to take the following defensive measures:

- Protect access to M1E controllers by a firewall blocking all remote/external access to Port 502.

Schneider Electric reports that Modicon M340, M580, Premium and Quantum users should take one or more of the following defensive measures:

- Enable protection based on an authentication to connect to PLC. This method relies on a feature named Application Password. Once enabled, password-based authentication is required whenever a user connects to change their application program;
- Enable protection relying on an input (M340, Premium, Quantum) or a key switch in the front panel (Quantum) to reject remote connection or run/stop commands; and
- Enable the “Access Control List protection,” where users are able to configure the restricted IP addresses that are pre-authorized to control the PLC.

For additional information, Schneider Electric has released a Cybersecurity Notification, which is available at the following location:

http://www.schneider-electric.com/en/download/document/SEVD-2017-065-01/

<http://www.schneider-electric.com/en/download/document/sevd-2017-065-01/>

NCCIC/ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

ICS-CERT also provides a section for control systems security recommended practices </ics/content/recommended-practices> on the ICS-CERT web page. Several recommended practices are available for reading and download, including Improving Industrial Control

Systems Cybersecurity with Defense-in-Depth Strategies.
</sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>, that is available for download from the ICS-CERT web site </ics/>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

VULNERABILITY OVERVIEW

AUTHENTICATION BYPASS BY CAPTURE-REPLAY CWE-294 <https://cwe.mitre.org/data/definitions/294.html>

Sensitive information is transmitted in cleartext in the Modicon Modbus protocol, which may allow an attacker to replay the following commands: run, stop, upload, and download.

CVE-2017-6034 has been assigned to this vulnerability. A CVSS v3 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:c/c:h/i:h/a:h>)

VIOLATION OF SECURE DESIGN PRINCIPLES CWE-657 <https://cwe.mitre.org/data/definitions/657.html>

The Modicon Modbus protocol has a session-related weakness making it susceptible to brute-force attacks.

CVE-2017-6032 has been assigned to this vulnerability. A CVSS v3 base score of 5.3 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:l/i:n/a:n>).

RESEARCHER

Eran Goldstein of CRITIFENCE reported the identified vulnerabilities.

BACKGROUND

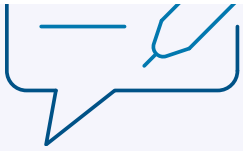
Critical Infrastructure Sectors: Critical Manufacturing, Dams, Defense Industrial Base, Energy, Food and Agriculture, Government Facilities, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater Systems

Countries/Areas Deployed: Worldwide

Company Headquarters Location: Paris, France

Vendor

- Schneider Electric



Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov