America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Schneider Electric Modicon PLCs

Last Revised: March 30, 2017 **Alert Code:** ICSA-17-089-02

CVSS v3 7.5

ATTENTION: Remotely exploitable/low skill level to exploit.

Vendor: Schneider Electric

Equipment: Modicon PLCs

Vulnerability: Predictable Value Range from Previous Values, Use of Insufficiently Random Values, Insufficiently Protected Credentials

AFFECTED PRODUCTS

The following versions of the Modicon M221, M241, and M251 programmable logic controllers (PLCs) are affected by a predictable value range from previous values vulnerability:

- Modicon M221, firmware versions prior to Version 1.5.0.0,
- Modicon M241, firmware versions prior to Version 4.0.5.11, and
- Modicon M251, firmware versions prior to Version 4.0.5.11.

The following versions of the Modicon M241 and M251 PLCs are affected by a use of insufficiently random values vulnerability:

- Modicon M241, firmware versions prior to Version 4.0.5.11, and
- Modicon M251, firmware versions prior to Version 4.0.5.11.

The following versions of the Modicon M241 and M251 PLCs are affected by an insufficiently protected credentials vulnerability:

- Modicon M241, all firmware versions, and
- Modicon M251, all firmware versions.

IMPACT

Successful exploitation of these vulnerabilities may allow a remote attacker to spoof or disrupt Transmission Control Protocol (TCP) connections, sniff sensitive account information, and gain unauthorized access to a current web session.

MITIGATION

Schneider Electric has released new firmware versions to address the predictable value range from previous values vulnerability and the use of insufficiently random values vulnerability, which are available through Schneider Electric's software update tool, SoMachine, Version 4.2, and SoMachineBasic, Version 1.5. Schneider Electric has not released a product to address the insufficiently protected credentials vulnerability; however, Schneider Electric has provided compensating controls to reduce the risk of exploitation.

SoMachineBasic, Version 1.5, is available at the following location:

http://www.schneider-electric.fr/fr/download/document/SOMBASAP15SOFT/

Schneider Electric has provided the following compensating controls to reduce the risk of exploitation of the insufficiently protected credentials vulnerability:

- Verify that the hardware and software infrastructure that the PLCs are integrated into (along with all organizational measures and rules covering access to the infrastructure) consider the results of the hazard and risk analysis, and are implemented according to best practices and standards such as ISA/IEC 62443.
- Limit traffic on the local network with managed switches
- Where possible, avoid using Wi-Fi networks, but when Wi-Fi is essential, use only secure communications (such as WPA2 encryption)
- Do not grant [network] access to unknown computers
- When remote access is essential, use secure methods such as Virtual Private Networks (VPNs), and ensure the remote access solution(s), as well as the remote computer(s) are kept up-to-date with the latest security patches.

Schneider Electric has released Security Notifications SEVD-2017-075-01, SEVD-2017-075-02, and SEVD-2017-075-03, which provide additional information about the identified vulnerabilities, mitigations, and compensating controls:

http://www.schneider-electric.com/en/download/document/SEVD-2017-075-01/
<http://www.schneider-electric.com/en/download/document/sevd-2017-075-01/>

http://www.schneider-electric.com/en/download/document/SEVD-2017-075-02/
<http://www.schneider-electric.com/en/download/document/sevd-2017-075-02/>

http://www.schneider-electric.com/en/download/document/SEVD-2017-075-03/
<http://www.schneider-electric.com/en/download/document/sevd-2017-075-03/>

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.

No known public exploits specifically target these vulnerabilities.

VULNERABILITY OVERVIEW

PREDICTABLE VALUE RANGE FROM PREVIOUS VALUES CWE-343

<https://cwe.mitre.org/data/definitions/343.html>

The affected products generate insufficiently random TCP initial sequence numbers that may allow an attacker to predict the numbers from previous values. This may allow an attacker to spoof or disrupt TCP connections.

CVE-2017-6030 has been assigned to this vulnerability. A CVSS v3 base score of 6.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L <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:l>).

USE OF INSUFFICIENTLY RANDOM VALUES CWE-330 <https://cwe.mitre.org/data/definitions/330.html>

The session numbers generated by the web application are lacking randomization and are shared between several users. This may allow a current session to be compromised.

CVE-2017-6026 has been assigned to this vulnerability. A CVSS v3 base score of 6.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/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:l/a:n>).

INSUFFICIENTLY PROTECTED CREDENTIALS CWE-522 <https://cwe.mitre.org/data/definitions/522.html>

Log-in credentials are sent over the network with Base64 encoding leaving them susceptible to sniffing. Sniffed credentials could then be used to log into the web application.

CVE-2017-6028 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/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:h/i:n/a:n>).

RESEARCHER

David Formby and Raheem Beyah of Georgia Tech and Fortiphyd Logic, Inc. reported the identified vulnerabilities.

BACKGROUND

Critical Infrastructure Sector(s): Critical Manufacturing, Food and Agriculture, 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