America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS ADVISORY

PLC Cycle Time Influences (Update A)

Last Revised: December 17, 2019 **Alert Code:** ICSA-19-106-03

1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low skill level to exploit/public exploits are available
- **Vendors:** ABB, Phoenix Contact, Schneider Electric, Siemens, WAGO
- **Equipment:** Programmable Logic Controllers
- **Vulnerability:** Uncontrolled Resource Consumption

2. UPDATE INFORMATION

This updated advisory is a follow-up to the original advisory titled ICSA-19-106-03 PLC Cycle Time Influences that was published April 16, 2019, on the ICS webpage on us-cert.gov.

3. RISK EVALUATION

High network load can consume CPU power in such a way that the normal operation of the device can be affected; that is, the configured cycle time can be influenced.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

4.1.1 ABB

- ABB 1SAP120600R0071 PM554-TP-ETH

4.1.2 PHOENIX CONTACT

- Phoenix Contact 2700974 ILC 151 ETH

--------- Begin Update A Part 1 of 2 ---------

- Phoenix Contact ILC 191 ETH 2TX

--------- End Update A Part 1 of 2 ---------

4.1.3 SCHNEIDER ELECTRIC

- Schneider Modicon M221

4.1.4 SIEMENS

- Siemens 6ES7211-1AE40-0XB0 Simatic S7-1211
- Siemens 6ES7314-6EH04-0AB0 Simatic S7-314
- Siemens 6ED1052-1CC01-0BA8 Logo! 8

4.1.5 WAGO

- WAGO 750-889 Controller KNX IP
- WAGO 750-8100 Controller PFC100
- WAGO 750-880 Controller ETH
- WAGO 750-831 Controller BACnet/IP

4.2 VULNERABILITY OVERVIEW

4.2.1 UNCONTROLLED RESOURCE CONSUMPTION CWE-400

<https://cwe.mitre.org/data/definitions/400.html>

Researchers have found some controllers are susceptible to a denial-of-service attack due to a flood of network packets.

CVE-2019-10953 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:n/i:n/a:h>).

4.3 BACKGROUND

ABB, Phoenix, Schneider Electric, Siemens, and WAGO are companies based in Europe that deploy their PLCs worldwide across the following critical infrastructure sectors: Chemical, Commercial Facilities, Critical Manufacturing, Dams, Energy, Food and Agriculture, Transportation Systems, and Water and Wastewater Systems.

4.4 RESEARCHER

Matthias Niedermaier (Hochschule Augsburg), Jan-Ole Malchow (Freie Universität Berlin), and Florian Fischer (Hochschule Augsburg) reported this vulnerability to CISA. Mikael Vingaard found and reported to CISA additional devices containing this vulnerability.

5. MITIGATIONS

PLC vendors have responded to queries about this report with the following mitigations:

5.1 ABB

ABB concludes the reported behavior is not a vulnerability but is due to a misconfiguration of the PLC watchdog, which was left in the default factory settings. This has led to a configuration that does not match the expectations expressed in the test cases and the result is the PLC not reacting as intended. This misconfiguration can be fixed by setting an appropriate combination of task priority, task cycle time, and watchdog settings. Please see the “Onboard Ethernet Handling in CPU Firmware” chapter (System Technology for AC500 V2 Products > System Technology of CPU and Overall System > Onboard Technologies > Ethernet > Ethernet Protocols and Ports for AC500 V2 Products > Onboard Ethernet Handling in CPU Firmware) for further guidance.

5.2 PHOENIX CONTACT

Phoenix Contact acknowledges this as a “known, won’t fix” issue for old products. Currently available products provide countermeasures to mitigate the impact on the safety-related functionality. Phoenix Contact urges users to adhere to the Application note 107913_en_01.

--------- Begin Update A Part 2 of 2 ---------

More information can be found in the VDE CERT advisory <https://cert.vde.com/en-us/advisories/vde-2018-012>.

--------- End Update A Part 2 of 2 ---------

5.3 SCHNEIDER ELECTRIC

Fixes are available in the Modicon M221 firmware v1.10.0.0 and the EcoStruxure Machine Expert – Basic v1.0 software (formerly SoMachine Basic) using either of the following options:

Use this link to download the Machine Expert Basic software.

Or run the Schneider Electric Software Update tool in order to download and install EcoStruxure Machine Expert – Basic v1.0 software.

For additional information, see the Schneider Electric security notice SEVD-2019-045-01.

Schneider Electric strongly recommends following industry cybersecurity best practices, such as:

- Physical controls should be in place so no unauthorized person would have access to the ICS and safety controllers, peripheral equipment, or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices it is intended.
- All methods of mobile data exchange with the isolated network (e.g., CDs, USB drives, etc.) should be scanned before use in terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.

5.4 SIEMENS

Siemens has investigated the vulnerability report on PLC cycle time influences and concludes the report does not demonstrate a valid vulnerability for Siemens PLCs.

5.5 WAGO

WAGO recommends users operate the devices in closed networks or protect them with a firewall against unauthorized access. Another recommended mitigation is to limit network traffic via the switch rate limit feature according to application needs.
Please also consult the product manuals on the WAGO website, as this is a known problem

for some devices. Links to product manuals and specific instructions about how to limit switch rates can be found in the VDE CERT advisory <https://cert.vde.com/de-de/advisories/vde-2018-013>.

5.6 CISA

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet <https://www.us-cert.gov/ics/alerts/ics-alert-10-301-01>.
- 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.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices <https://www.us-cert.gov/ics/recommended-practices> on the ICS webpage on us-cert.gov <https://www.us-cert.gov/ics>. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies <https://www.us-cert.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.gov <https://www.us-cert.gov/ics> in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.us-cert.gov/ics/tips/ics-tip-12-146-01b>.

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

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- ABB
- PHOENIX CONTACT
- Schneider Electric
- Siemens
- WAGO

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>