SA-CDS-20171207-001: Critical 3S CODESYS vulnerabilities in WAGO PFC200 Series

Publication Date: 2017-12-07
Last Update: 2017-12-07
Version: V1.0
Severity: Critical

Affected Products

The following 3S CoDeSys Runtime versions of the PFC200 Series are affected:

- CoDeSys Version 2.3.X
- CoDeSys Version 2.4.X

The affected CoDeSys Runtime version is part of WAGO PFC200 Firmware <= 02.07.07(10).

Affected PFC200-Devices:
•750-8202
•750-8202/025-000
•750-8202/025-001
•750-8202/025-002
•750-8202/040-001
•750-8203
•750-8203/025-000
•750-8204
•750-8204/025-000
•750-8206
•750-8206/025-000
•750-8206/025-001
•750-8207
•750-8207/025-000
•750-8207/025-001
•750-8208
•750-8208/025-000

Impact

A remote attacker who could successfully exploit the vulnerabilities could get unauthorized access to the PLC for performing privileged operations to the file system without authentication.

Description

The vulnerability based on the security problems which were reported by Reid Wightman [2].
It is possible to execute different unauthenticated remote operations because of the CoDeSys Runtime application which is available via network by default (port 2455).
This open port 2455 is required to transfer the PLC application to the device and which has to be closed after initial commissioning.
Otherwise, an attacker could execute some unauthenticated commands by sending specially-crafted TCP packets to port 2455.
The following operations are possible, for example:

- An attacker could read, write and delete arbitrary files.
- An attacker could manipulate the PLC application during runtime.

Vulnerability Characterization

The vulnerability based on the report of the ICS-CERT [2].

Improper Authentication

The CoDeSys Runtime does not require users to authenticate for performing critical operations.
Therefore an attacker could obtain administrative privileges on the device.
This could allow the attacker to compromise the availability, integrity, and confidentiality of the device.

Vulnerability Details

- Exploitability: This vulnerability could be exploited remotely.
- Existence of Exploit: Exploits that target this vulnerability are publicly available.
- Difficulty: An attacker with a low skill would be able to exploit this vulnerability.

Solution

Security-Patch will be available with FW11.

Mitigation

- Network access to the device should be restricted.
- Do not directly connect the device to the internet.
- Close the programming network port 2455 via WBM.

Reported

T. Weber of the SEC Consult Vulnerability Lab reported the vulnerability to WAGO.

Additional Resources

[1] https://www.sec-consult.com/en/blog/advisories/wago-pfc-200-series-critical-codesys-vulnerabilities/index.html
[2] ICS-CERT, Advisory (ICSA-13-011-01), 3S CoDeSys Vulnerabilities: https://ics-cert.us-cert.gov/advisories/ICSA-13-011-01
[3] WAGO Website, http://global.wago.com/en/products/product-catalog/components-automation/security-notes/index.jsp

Disclaimer

http://global.wago.com/en/wago/impressum/software-user-agreement/index.jsp