SSA-197012: Vulnerabilities in SICLOCK central plant clocks

Publication Date: 2018-07-03
Last Update: 2018-07-03
Current Version: V1.0
CVSS v3.0 Base Score: 9.8

SUMMARY

SICLOCK TC devices are affected by multiple vulnerabilities that could allow an attacker to cause Denial-of-Service conditions, bypass the authentication, and modify the firmware of the device or the administrative client.

SICLOCK TC devices are in a phase out process. Siemens recommends mitigations to reduce the risk.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SICLOCK TC100: All versions	See recommendations from section Workarounds and Mitigations
SICLOCK TC400: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Provide redundant time sources and implement plausibility checks for the time information in critical plant controllers.
- Protect network access to the affected devices with appropriate measures, e.g. protect SICLOCK TC devices with firewalls to reduce the risk.

  It is recommended to filter traffic to all ports excluding those needed for time synchronization. If time synchronization is performed using NTP, then port 123/udp must be opened on the firewall. If time synchronization is performed using SIMATIC time synchronization, then port 22223/udp and port 22224/udp must be opened on the firewall.

  For configuring parameters, it is recommended to use a direct connection to the SICLOCK TC.
- Apply the cell protection concept, and apply defense-in-depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

The SICLOCK product family offers components for synchronizing the time in industrial plants and systems. The SICLOCK central plant clocks evaluate the clock time information received from the radio receiver and supply all connected network nodes with precise and uniform time information.

In the event of failure or loss of reception from the primary time source, the central plant clock ensures stable continuation of the clock time, and tracking of the system time without time jumps as soon as reception is restored. Available products are the SICLOCK TC100 for smaller plants and the SICLOCK TC400.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2018-4851

An attacker with network access to the device, could cause a Denial-of-Service condition by sending certain packets to the device, causing potential reboots of the device. The core functionality of the device could be impacted. The time serving functionality recovers when time synchronization with GPS devices or other NTP servers are completed.

The security vulnerability could be exploited by an attacker with network access to the affected devices. Successful exploitation requires no user interaction. The vulnerability could impact the availablity of the device, and could impact the integrity of the time service functionality of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.1
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:P/RL:T/RC:C

Vulnerability CVE-2018-4852

An attacker with network access to the device could potentially circumvent the authentication mechanism, if he is able to obtain certain knowledge specific to the attacked device.

The security vulnerability could be exploited by an attacker with network access to the affected devices. Furthermore, the attacker must obtain certain knowledge that is specific to the device. Successful exploitation requires no user interaction. The vulnerability could allow an attacker to read and modify the device configuration.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.4
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:T/RC:C

Vulnerability CVE-2018-4853

An attacker with network access to port 69/udp could modify the firmware of the device.

The security vulnerability could be exploited by an attacker with network access to the affected devices. Successful exploitation requires no user interaction. The vulnerability could allow an attacker to run his own code on the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C

Vulnerability CVE-2018-4854

An attacker with network access to port 69/udp could modify the administrative client stored on the device. If a legitimate user downloads and executes the modified client from the affected device, then he could obtain code execution on the client system.

The security vulnerability can be exploited by an attacker with network access to the device. User interaction is required in order for the attack to compromise the client system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.6
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:T/RC:C

Vulnerability CVE-2018-4855

Unencrypted storage of passwords in the client configuration files and during network transmission could allow an attacker in a privileged position to obtain access passwords.

The security vulnerability could be exploited by an attacker in a privileged network position which allows intercepting the communication between the affected device and the administrative client. The user must invoke a session between the administrative client and the device. The vulnerability could allow reading the access passwords for the devices.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C

Vulnerability CVE-2018-4856

An attacker with administrative access to the device's management interface could lock out legitimate users. Manual interaction is required to restore the access of legitimate users.

The security vulnerability could be exploited by an attacker with network access to the affected devices. Furthermore, the attacker must be authenticated to the management interface before executing the attack. Successful exploitation requires no user interaction.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	2.7
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L/E:P/RL:T/RC:C

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-07-03): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.