SIEMENS-SSA-625789: Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU

Publishing Date	2011-06-10
Last Update	2011-09-12
Current Version	V2.1
CVSS Overall Score	6.5

SUMMARY:

Security experts have examined the SIMATIC S7-1200 Programmable Logic Controller (PLC). This research has revealed some weaknesses in the SIMATIC S71200 CPU communication and authentication functions. Once the automation network is compromised it is possible to demonstrate the following weaknesses using a remote exploit:

- Trigger CPU functions by record and playback of legitimate network communication
- Place CPU in stop/defect state by causing a communications error

A remote exploit is a type of attack that can be launched from one computer against another computer across a network. For example, a PC with access to the automation network could be used to launch a remote exploit against a PLC.

The weaknesses are closed with a firmware update V 2.0.3. For the second weakness (communications error), a temporary work-around is also available: if the Web server on the S7-1200 is disabled, the weakness cannot be exploited.

AFFECTED COMPONENTS

- Trigger CPU functions: SIMATIC S7-1200 CPU firmware version prior to V 2.0.3
- Place CPU in stop/defect state: SIMATIC S7-1200 CPU firmware version V 2.0.2

DESCRIPTION

Siemens CERT was notified by ICS-CERT about certain weaknesses in the SIMATIC S7-1200 CPU product:

Trigger CPU functions by record and playback

Prior to applying the latest firmware update (V 2.0.3) it was possible to record communication between the engineering software and the controller using available open source tools and to replay the communication to the controller at a later time. This made it possible to execute any previously recorded commands issued by the engineering software to the PLC at a later time (e.g. set controller to STOP). This was true whether or not the controller had a password configured.

Place CPU in stop/defect state by causing a communications error

Prior to applying the latest firmware update (V 2.0.3) it was possible to place the controller in the stop/defect state by causing a communications error (e.g., by running a network scan sending malformed HTTP traffic at high rate). Thus a communications error occurred in the Web server interface of the S7-1200 causing the controller to enter the stop/defect state. In automation applications, the stop/defect state is a defined state in which the external process (e.g. the machine) is stopped, comparable to a power loss.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://www.first.org/cvss/).

Trigger CPU functions by Record and Playback

CVSS Base Score 7.9
CVSS Temporal Score 6.5
CVSS Overall Score 6.5 (AV:A/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:O/RC:C)

Mitigating Factors

- An attacker must have access to the automation network where the CPU is located.
- If controllers are configured with unique passwords, replaying the traffic between the engineering software and one controller to a second controller has no effect.

Place CPU in stop/defect state by applying a network scanner

CVSS Base Score 5.7
CVSS Temporal Score 4.7
CVSS Overall Score 4.7 (AV:A/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:O/RC:C)

Mitigating Factors

- An attacker must have access to the automation network where the CPU is located
- The Web server must be enabled for this vulnerability to be exposed

SOLUTION

Updates correcting both of these system behaviors are now available in firmware update V 2.0.3 [5].

As a temporary measure to protect against the second weakness (communications error), until the customer has completed the firmware update to V 2.0.3, Siemens recommends that the Web server be disabled. The Web server was first introduced into the S7-1200 in firmware version 2.0.2. The ability to disable the Web server is available in TIA Portal Version 11.

In addition, it is important to ensure the automation network is protected from unauthorized access using the strategies suggested in the PCS7 security concept [1] document.

If the firmware has been updated but no controller password has been set, replay attacks are still possible due to the nature of clear text industrial automation protocols. Therefore Siemens recommends a unique, strong password protection is applied to all controllers in an automation solution.

ADDITIONAL INFORMATION

As industrial automation protocols frequently are clear text, they are susceptible to standard attacks at network level such as replay or information extraction. Systems engineers must always consider appropriate security mechanisms in open communications that apply to each network hierarchy level. Usually this is achieved using secure network switches or gateways with firewall functions. Siemens offers all users and plant operators extensive support for these tasks. By design, Siemens supports an open communications architecture and recommends that customers check their adherence to the security precautions recommended in the PCS7 security concept [1].

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts in this issue:

- Dillon Beresford from NSS Labs for his investigations
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts

ADDITIONAL RESOURCES

[1] Siemens Industry Automation Security Manual:
http://support.automation.siemens.com/WW/view/en/28580051

[2] Further information about the SIMATIC S7-1200 CPU can be found at the Siemens Website:
http://www.automation.siemens.com/mcms/programmable-logiccontroller/en/simatic-s7-controller/s7-1200/Pages/Default.aspx

[3] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens CERT:
http://www.siemens.com/cert

[4] Additional Information:
http://support.automation.siemens.com/WW/view/en/50428932

[5] Link to firmware update page:
http://support.automation.siemens.com/WW/view/en/41886031/130000

HISTORY DATA

V1.0 (2011-06-10): Publication Date
V2.0 (2011-07-05): Modification of CVSS scoring, solution and version information
V2.1 (2011-09-12): Update of solution section by removing mentioning of air gap

DISCLAIMER

See: http://www.siemens.com/terms_of_use