SSA-237894: Vulnerability in SIMATIC PCS 7

Publication Date 2015-04-23
Last Update 2015-09-28
Current Version 1.1
CVSS Overall Score 5.3

Summary:

The latest updates for SIMATIC PCS 7 fix a vulnerability that could allow an attacker to use password hashes for authentication under certain conditions.

AFFECTED PRODUCTS

SIMATIC PCS 7: All versions < V8.1 SP1

DESCRIPTION

SIMATIC PCS 7 is a distributed control system (DCS) for supervisory control and data acquisition of (SCADA) systems. It is used to monitor and control physical processes involved in industry and infrastructure on a large scale and over long distances.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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 Description (CVE-2015-2823)

If attackers obtain password hashes of SIMATIC WinCC users, they could possibly use the hashes to authenticate themselves.

CVSS Base Score	6.8
CVSS Temporal Score	5.3
CVSS Overall Score	5.3 (AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Mitigating factors

The attacker must be able to obtain a password hash.

Siemens recommends operating the affected products only within trusted networks [3].

SOLUTION

Siemens provides Service Pack 1 [1] for SIMATIC PCS 7 V8.1 and SIMATIC WinCC V7.2 Upd11 [2] for SIMATIC PCS 7 V8.0 SP2 which fix the vulnerability. Siemens recommends customers to update to the new fixed versions.

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks Ilya Karpov from Positive Technologies for coordinated disclosure of this vulnerability.

ADDITIONAL RESOURCES

[1] Information on how to obtain Service Pack 1 for SIMATIC PCS 7 V8.1 can be found here:
https://support.industry.siemens.com/cs/ww/en/view/108463041

[2] Update 11 for SIMATIC WinCC V7.2 can be obtained here:
https://support.industry.siemens.com/cs/de/en/view/109478834

[3] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[4] Information about Industrial Security by Siemens:
http://www.siemens.com/industrialsecurity

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

HISTORY DATA

V1.0 (2015-04-23): Publication Date
V1.1 (2015-09-28): Added fix information for PCS 7 V8.0 SP2

DISCLAIMER