SSA-628113: Open Debugging Port in CP 1616 and CP 1604

Publication Date 2013-02-13
Last Update 2013-02-18
Current Version V1.1
CVSS Overall Score 8.3

Summary:

CP 1604 and CP 1616 interface cards have a debugging interface that is enabled by default and remotely accessible. This debugging interface allows Denial-of-Service, loss of confidentiality and remote code execution on the installed system. Siemens addresses this issue by a firmware update.

AFFECTED PRODUCTS

- CP 1616 (6GK1 161-6AA00, 6GK1 161-6AA01, 6GK1 161-6AA02)
- CP 1604 (6GK1 160-4AA00, 6GK1 160-4AA01)
- CP 1604 Microbox Package (6GK1 160-4AU00)
- CP 1616 Onboard card of SIMATIC IPCs (6GK1 160-4AU01)

DESCRIPTION

The CP 1616 and CP 1604 interface cards are used for connecting Personal Computers and PCI-104 systems to PROFINET IO. A debugging interface has been enabled in these products by default. This allows Denial-of-Service attacks, loss of confidentiality and remote code execution by sending specially crafted packets to network port 17185/UDP.

Detailed information about the vulnerability 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

A debugging interface is enabled by default on the affected devices. It allows Denial-of-Service attacks, loss of confidentiality and remote code execution.

CVSS Base Score	10.0
CVSS Temporal Score	8.3
CVSS Overall Score	8.3 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)

Mitigating factors:

The attacker must have network access to the affected system on UDP network port 17185. Siemens recommends operating the devices only within trusted networks [2].

SOLUTION

Siemens provides a firmware update for both affected products which closes the debugging port and protects against all mentioned attacks [1]. Siemens recommends installing the update as soon as possible.

The affected software components are implemented under the assumption of running in a protected IT environment. Siemens strongly recommends to protect systems according to recommended security practices in [4] and to configure the environment according to operational guidelines [2].

ACKNOWLEDGEMENT

Siemens thanks Christopher Scheuring and Jürgen Bilberger from Daimler TSS GmbH for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

1. The firmware update V2.5.2 is published on the following web site:
   http://support.automation.siemens.com/WW/view/en/67634096
2. An overview of the operational guidelines for Industrial Security (with the cell protection concept):
   http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
3. Information about Industrial Security by Siemens:
   http://www.siemens.com/industrialsecurity
4. Recommended security practices by US-CERT:
   http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
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 (2013-02-13): Publication Date
V1.1 (2013-02-18): Added acknowledgement

DISCLAIMER