SIEMENS-SSA-460621: Security Vulnerability in Siemens WinCC Flexible Runtime Loader Could Allow Memory Corruption

Publishing Date	2011-08-29
Last Update	2011-09-05
Current Version	V1.2
CVSS Overall Score	7.5

Summary:
A vulnerability was disclosed in the WinCC flexible runtime loader, which is a part of WinCC flexible. If a manipulated packet is sent to the listening port of the WinCC flexible runtime loader, an attacker may create a memory corruption condition due to insufficient input sanitization.

AFFECTED SOFTWARE

- SIMATIC WinCC flexible (versions: 2005, 2005 SP1, 2007, 2008, 2008 SP1, 2008 SP2)
- TIA Portal V11

DESCRIPTION

A vulnerability was disclosed in the WinCC flexible runtime loader. If the transfer mode is activated, the WinCC flexible runtime loader listens on TCP port 2308. However, it does not sanitize its inputs before processing them. If a manipulated packet is sent to the port, an attacker may enforce a memory corruption leading to potential code execution or a denial of service of the WinCC flexible runtime loader.

VULNERABILITY CLASSIFICATION

Details of the security vulnerabilities are outlined in the following. The vulnerability classification has been performed by using the CVSSv2 scoring system (http://www.first.org/cvss/).

CVSS Base Score	7.9
CVSS Temporal Score	7.5
CVSS Overall Score	7.5 (AV:A/AC:M/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C)

Mitigating Factors

The attacker has to have access to the network where the WinCC flexible runtime loader is located. The transfer mode has to be turned on in the WinCC flexible runtime loader.

SOLUTION

The affected software components are implemented according to the assumption of running in a protected IT environment. Siemens strongly recommends to protect systems according to recommended security practices in [2] and to configure the environment according to operational guidelines [3].

ACKNOWLEDGEMENT

Siemens thanks

- Billy Rios and Terry McCorkle for reporting the vulnerability
- the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting and coordination efforts.

ADDITIONAL RESOURCES

[1] Further information about WinCC flexible can be found at the Siemens Website: http://www.automation.siemens.com/mcms/human-machine-interface/en/visualization-software/wincc-flexible/Pages/Default.aspx

[2] Recommended security practices by US-CERT:
http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

[3] PCS7 Security concept:
http://support.automation.siemens.com/WW/view/en/22229786

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

HISTORY DATA

V1.0 (2011-08-29): Internal Publication Date
V1.1 (2011-08-30): Internal Use Highlighted
V1.2 (2011-09-05): External Publication, update of CVSS Score

DISCLAIMER

