SIEMENS-SSA-630126: Multiple Vulnerabilities in Siemens Tecnomatix FactoryLink

Publishing Date	2011-03-30
Last Update	2011-03-30
Current Version	V1.0
CVSS Overall Score	8.7

Summary:
Multiple vulnerabilities have been reported in the Siemens Tecnomatix FactoryLink product. Together with the vulnerabilities, exploit code has been published. Siemens AG has released software updates that address these vulnerabilities. One of the reported vulnerabilities can be closed by proper configuration.

AFFECTED SOFTWARE

- Tecnomatix FactoryLink 8.0.1
- Tecnomatix FactoryLink 8.0.2
- Tecnomatix FactoryLink 7.5.2
- FactoryLink ECS 6.6.1

DESCRIPTION

Siemens CERT became aware of vulnerabilities in SCADA products (for details see [1] and [2]). The publication [2] contains details of the vulnerabilities as well as proof-of-concept exploit code. The affected products include also Tecnomatix FactoryLink, which is a product from the Siemens Industry sector.

Analysis by the Siemens development team has been performed with the outcome that five of the six reported alleged vulnerabilities have been closed through patches released on 2011-03-25. One alleged vulnerability does not require a bug fix as this can be fixed by a configuration adjustment recommended by Siemens (see the recommendations in the Readme files of the patches [3]).

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/).

Vulnerability #1

Bad data sent via the network may cause CSService (a FactoryLink service) to crash or have abnormal behavior. This is caused by buffer overrun conditions. This vulnerability affects only Tecnomatix Factorylink version 8.0.1 and 8.0.2.

CVSS Base Score	9.0
CVSS Temporal Score	7.8
CVSS Overall Score	7.8 (AV:N/AC:L/Au:N/C:P/I:P/A:C/E:H/RL:OF/RC:C)

Vulnerability #2

CSService allows arbitrary files to be downloaded from the server. This vulnerability affects only Tecnomatix Factorylink version 8.0.1 and 8.0.2.

CVSS Base Score	7.8
CVSS Temporal Score	6.8
CVSS Overall Score	6.8 (AV:N/AC:L/Au:N/C:C/I:N/A:N/E:H/RL:OF/RC:C)

Vulnerability #3

Bad data sent via the network may cause VRN (server communications task) to crash or have abnormal behavior. A parse failure of this data causes the stack to be overwritten. A mitigating factor is to configure the system properly (see the recommendations in the Readme files of the patches [3]), which improves the CVSS Authentication level.

CVSS Base Score	10.0
CVSS Temporal Score	8.7
CVSS Overall Score	8.7 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)

Vulnerability #4

Bad data sent via the network may cause VRN (Server communications task) to crash or have abnormal behavior. A parse failure of this data causes a stack overflow. A mitigating factor is to configure the system properly (see the recommendations in the Readme files of the patches [3]), which improves the CVSS Authentication level.

CVSS Base Score	7.8
CVSS Temporal Score	6.8
CVSS Overall Score	6.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:H/RL:OF/RC:C)

Vulnerability #5

Bad data sent via the network may cause CSService, connsrv and datasrv to crash or have abnormal behavior. This is due to NULL pointer dereferencing.

CVSS Base Score	7.8
CVSS Temporal Score	6.8
CVSS Overall Score	6.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:H/RL:OF/RC:C)

Mitigating Factors

An attacker must have access to the network, where the Tecnomatix FactoryLink application is located. A mitigating factor for the vulnerabilities #3 and #4 is to configure the system properly (see the recommendations in the Readme files of the patches [3]).

SOLUTION

Siemens has provided patches for closing the vulnerabilities. Siemens strongly recommends the patches to be installed as soon as possible.

- Tecnomatix FactoryLink
  The patches for the different FactoryLink versions are available at http://www.usdata.com/sea/factorylink/en/p_nav5.asp

- Workaround
  N/A

The security issue #5 reported in [2] is due to improper configuration. Incorrect configuration allows the vrn.exe file to download arbitrary files without authorization. It can be solved by applying the correct configuration to the system (see the recommendations in the Readme files of the patches [3]).

ADDITIONAL RESOURCES

[1] ICS-CERT Alert:
http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-080-01.pdf

[2] Bugtraq entry of vulnerability publication:
http://seclists.org/bugtraq/2011/Mar/187

[3] The patches for the different Tecnomatix versions are available at:
http://www.usdata.com/sea/factorylink/en/p_nav5.asp

[4] Further information about Tecnomatix can be found at the Siemens Website:
http://www.usdata.com/sea/factorylink/en/p_nav1.html

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

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

HISTORY DATA

V1.0 (2011-03-30): Publication Date

DISCLAIMER

