

SSA-850510: Siemens Tecnomatix FactoryLink Multiple ActiveX Vulnerabilities

| | |
|--------------------|------------|
| Publishing Date | 2011-12-09 |
| Last Update | 2012-01-19 |
| Current Version | V1.2 |
| CVSS Overall Score | 7.7 |

Summary:

Two vulnerabilities were disclosed in methods of an ActiveX object installed by Tecnomatix FactoryLink. If a user opens a manipulated website, an attacker may execute arbitrary code on the system or write certain information to the system. Siemens provides updates for closing the vulnerabilities, which restrict the malicious usage of ActiveX controls.

AFFECTED SOFTWARE

- Siemens Tecnomatix FactoryLink V8.0.2.54
- Siemens Tecnomatix FactoryLink V7.5.217 (V7.5 SP2)
- Siemens Tecnomatix FactoryLink V6.6.1 (V6.6 SP1)

DESCRIPTION

Tecnomatix FactoryLink installs an ActiveX object with methods that allow the execution of code and overwriting files on the victim system. When browsing maliciously manipulated HTML files with Internet Explorer, an attacker may execute arbitrary code on the remote system or place information on the system.

The first vulnerability is triggered by inputting a long string to a parameter causing a buffer overflow, thus allowing execution of arbitrary code.

The second vulnerability is triggered by inputting arbitrary data, causing a file save to a freely specifiable location. In this way, attackers could damage the victim's system.

At the present time, we are not aware of active exploitation of our product by the vulnerabilities.

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.

| | |
|---------------------|---|
| CVSS Base Score | 9.3 |
| CVSS Temporal Score | 7.7 |
| CVSS Overall Score | 7.7 (AV:N/AC:M/Au:N/C:I/C/A:C/E:F/RL:OF/RC:C) |

Mitigating Factors

The vulnerability can only be exploited if ActiveX controls are enabled in Internet Explorer. ActiveX controls are deactivated by default in Internet Explorer. In addition, the user has to invoke specifically manipulated HTML files, e.g. by accessing Internet content, that trigger the vulnerability.

SOLUTION

Siemens provides updates for closing the vulnerabilities that restrict the malicious usage of ActiveX controls. Siemens strongly recommends to install the updates as soon as possible.

- Tecnomatix FactoryLink buffer overflow

The patches for the various Tecnomatix versions are also available at

http://www.usdata.com/sea/factorylink/en/p_nav5.asp

The security updates listed below are for FactoryLink versions 8.0.2, 7.5.2 and 6.6.1. These represent the last maintenance releases of the last 3 major releases of FactoryLink:

- SecurityUpdate802.305
- SecurityUpdate752.1401
- SecurityUpdate661.305

If you are running a different version of FactoryLink and require this security update, we recommend you to upgrade to one of these versions of FactoryLink.

- Tecnomatix FactoryLink file overwrite

Siemens also recommends installing the Microsoft update referenced in the Microsoft Security Advisory 2562937:

<http://technet.microsoft.com/en-us/security/advisory/2562937>

- Workaround for both vulnerabilities

Deactivate ActiveX controls in Internet Explorer.

ACKNOWLEDGEMENT

Siemens thanks

- Researcher Kuang-Chun Hung of the Security Research and Service Institute of the Information and Communication Security Technology Center (ICST) for reporting the vulnerability.
- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting and coordination efforts.

ADDITIONAL RESOURCES

[1] The patches for the various Tecnomatix versions are available at

http://www.usdata.com/sea/factorylink/en/p_nav5.asp

[2] Further information about Tecnomatix can be found at the Siemens Website:

http://www.usdata.com/sea/factorylink/en/p_nav1.html

[3] Recommended security practices by US-CERT:

http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

[4] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

productcert@siemens.com

<http://www.siemens.com/cert/advisories>

HISTORY DATA

V1.0 (2011-12-07): Internal publication date

V1.1 (2011-12-09): External publication date

V1.2 (2012-01-19): Updated affiliation

DISCLAIMER

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