# SSA-864051: Multiple Vulnerabilities in WinCC 7.0 SP3

| | |
|---|---|
| Publishing Date | 2012-09-10 |
| Last Update | 2012-09-10 |
| Current Version | V1.0 |
| CVSS Overall Score | 7.0 |

Summary:

WinCC WebNavigator is susceptible to twelve vulnerabilities, which compromise (depending on the vulnerability) the confidentiality, integrity or availability of the affected system over the network. WebNavigator is part of WinCC 7.0.

## AFFECTED PRODUCTS

The vulnerabilities exist in the "WebNavigator" component of WinCC 7.0 SP3 and earlier.

As WinCC 7.0 is part of SIMATIC PCS7 V8, this product is also affected by these vulnerabilities.

## DESCRIPTION

The WebNavigator component of WinCC gives the users the possibility to control their plants via the web browser with the same look-and-feel like local operator stations. However, the WebNavigator application is vulnerable to various attacks:

- Reflected Cross Site Scripting was found in POST parameters, GET parameters and referrers. If this attack is successful, the attacker can take over the WebNavigator session with the victim's rights.
- Cross Site Request Forgery is related to the Cross Site Scripting vulnerability and works in a similar way: If a victim clicks on a malicious link, actions can be triggered in the browser, where WebNavigator is running.
- Arbitrary file reading over the web interface was possible on the web folder on certain directories and files. An attacker with access to the WebNavigator web server can read data like log files and configuration files, which might have sensitive content.
- SQL injection and information disclosure in SOAP messages gives an attacker the opportunity to extract potentially sensitive data from the database.
- An ActiveX control can be exploited by a malicious web site to transmit the username and password of an authenticated user to the attacker.

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 1 (CVE-2012-3031)

Reflected Cross Site Scripting often starts with a phishing mail or similar social engineering. With this, an authenticated user could be tricked to click a malicious link. Due to the Cross Site Scripting vulnerability, this action may start a java script in the victim's browser which can have malicious behaviour, e.g. steal his session cookie.

Preconditions: the attacker must know the IP address or hostname of WebNavigator and must be able to convince the victim to click on a link.

| | |
|---|---|
| CVSS Base Score | 8.3 |
| CVSS Temporal Score | 6.5 |
| CVSS Overall Score | 6.5 (AV:N/AC:M/Au:N/C:P/I:P/A:C/E:POC/RL:OF/RC:C) |

Vulnerability 2 (CVE-2012-3028)

Cross Site Request Forgery is very similar to the Cross Site Scripting vulnerability (see above). It also starts with an authenticated user clicking on a malicious link. However, this vulnerability also works if the user has disabled scripting in his browser.

Preconditions: the attacker needs to have detailed information about the project for successfully triggering actions. He also needs to know the WebNavigator IP address or hostname and he must convince the victim to click on the link.

| | |
|---|---|
| CVSS Base Score | 7.8 |
| CVSS Temporal Score | 6.7 |
| CVSS Overall Score | 6.7 (AV:N/AC:M/Au:N/C:N/I:P/A:C/E:POC/RL:W/RC:C) |

Vulnerability 3 (CVE-2012-3030)

The WebNavigator web server does not only serve the WebNavigator web application, but also further files. If an attacker knows or guesses the right path and/or file name, he can read these files. This vulnerability is called “forceful browsing”.

Depending on the data, this can be a breach of confidentiality. Moreover, the attacker might use the information of configuration files or log files to launch or improve further attacks.

Precondition: to exploit this vulnerability, the attacker needs access to the web server and needs to know/guess the path and file name.

| | |
|---|---|
| CVSS Base Score | 5.0 |
| CVSS Temporal Score | 3.9 |
| CVSS Overall Score | 3.9 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C) |

Vulnerability 4 (CVE-2012-3032)

WebNavigator uses part of the content of SOAP messages to create SQL database queries. If an attacker sends a specially crafted SOAP message to the server, the resulting SQL queries might read or write more data in the database than originally intended.

Precondition: to exploit this vulnerability, the attacker needs access to the web server.

| | |
|---|---|
| CVSS Base Score | 9.0 |
| CVSS Temporal Score | 7.0 |
| CVSS Overall Score | 7.0 (AV:N/AC:L/Au:N/C:P/I:P/A:C/E:POC/RL:OF/RC:C) |

Vulnerability 5 (CVE-2012-3034)

WebNavigator uses ActiveX controls in the user’s browser. The methods of these ActiveX controls can be called by any web site this user visits. By maliciously parameterizing this method, the attacker can gain access to username and password of the legitimate user.

Precondition: to exploit this vulnerability, the attacker needs access to the web server.

| | |
|---|---|
| CVSS Base Score | 8.3 |
| CVSS Temporal Score | 6.5 |
| CVSS Overall Score | 6.5 (AV:N/AC:M/Au:N/C:C/I:P/A:P/E:POC/RL:OF/RC:C) |

Mitigating factors:

For vulnerabilities 1, 2 and 5, the attacker must trick the user to click on a malicious link while being logged into WebNavigator. Users with good security awareness are more likely to avoid this. Moreover, the attacker needs to know the URL of the specific WebNavigator installation.

Vulnerability 3 and vulnerability 4 can only be exploited if the attacker has access to the WebNavigator web interface.

## SOLUTION

Siemens provides an update for WinCC 7.0 SP3, which fixes vulnerabilities 1, 3, 4 and 5 and recommends installing the patch. It is recommended to restrict access to WebNavigator e.g. with a firewall or VPN gateway or to operate the service only within trusted networks.

No patch is yet available for vulnerability 2. Siemens recommends:

- Do not interact with other internet related services while being logged in
- Log out when WebNavigator is not needed any more

This WinCC 7.0 SP3 update should also be applied by SIMATIC PCS7 users running PCS 7 V8.0 Update 1.

## ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Denis Baranov Sergey Bobrov, Artem Chaykin, Vladimir Kochetkov, Pavel Toporkov, Timur Yunusov from Positive Technologies

## ADDITIONAL RESOURCES

1. The patch can be found on this site:
   http://support.automation.siemens.com/WW/view/en/63472422
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 (2012-09-10): Publication Date

## DISCLAIMER