ICS-CERT ADVISORY

ICSA-12-256-01-SIEMENS WINCC WEBNAVIGATOR MULTIPLE VULNERABILITIES

September 12, 2012

OVERVIEW

Siemens has reported multiple vulnerabilities in the Siemens WinCC WebNavigator application. These vulnerabilities were originally reported directly to Siemens by Positive Technologies. Siemens has produced an update that mitigates these vulnerabilities. These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

Siemens reports that these vulnerabilities affect the WebNavigator component of the following versions of WinCC:

- WinCC 7.0 SP3 and earlier.

IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to access sensitive data or possibly take over the WebNavigator session with the same rights as the victim.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

WinCC/Web Navigator is a WinCC option that provides a Web interface for the Siemens SIMATIC WinCC Human Machine Interface (HMI). SIMATIC WinCC performs the following tasks: process visualization, operator control of the process, alarm display, process value and alarm archiving, and machine parameter management. This software is used in many industries, including food and beverage, water and wastewater, oil and gas, and chemical.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

1. REFLECTED CROSS SITE SCRIPTING[a]

An attacker can use social engineering to trick an authenticated user into clicking a malicious link. This action may execute a java script in the victim's browser, which can have malicious behavior such as stealing a session cookie.

CVE-2012-3031[b] has been assigned to this vulnerability. A CVSS v2 base score of 8.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:P/A:C).[c]

2. CROSS SITE REQUEST FORGERY[d]

Cross site request forgery is similar to the cross site scripting vulnerability (see above). It can also be triggered by an authenticated user clicking on a malicious link. However, this vulnerability also works if the user has disabled scripting in his or her browser.

CVE-2012-3028[e] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:P/A:C). [f]

a. CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), http://cwe.mitre.org/data/definitions/79.html, Web site last accessed September 12, 2012.

b. NVD,http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3031 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:P/I:P/A:C), Web site last accessed September 12, 2012.

d. CWE-352: Cross-Site Request Forgery (CSRF), http://cwe.mitre.org/data/definitions/352.html, Web site last accessed September 12, 2012.

e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3028 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:N/I:P/A:C), Web site last accessed September 12, 2012.

3. FORCEFUL BROWSING[g]

If an attacker knows or guesses the right path and/or file name, he or she can read files on the system that hosts WebNavigator.

CVE-2012-3030[h] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).[i]

4. SQL INJECTION[j]

If an attacker sends a specially crafted SOAP (Simple Object Access Protocol) message to the server, the resulting SQL queries might read or write more data in the database than originally intended.

CVE-2012-3032[k] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:P/A:C). [l]

5. ACTIVEX[m]

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 using specially crafted parameters with these methods, an attacker can gain access to the username and password of a legitimate user.

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

CVE-2012-3034[n] has been assigned to this vulnerability. A CVSS v2 base score of 8.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:P/A:P).[o]

g. CWE-425: Direct Request ('Forced Browsing', http:/cwe.mitre.org/data/definitions/425.html, Web site last accessed September 12, 2012.

h. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3030 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

i. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N), Web site last accessed September 12, 2012.

j. CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), http://cwe.mitre.org/data/definitions/89.html, Web site last accessed September 12, 2012.

k. NVD,http:/web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3032, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

l. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:P/A:C), Web site last accessed September 12, 2012.

m. CWE-618: Exposed Unsafe ActiveX Method, http://cwe.mitre.org/data/definitions/618.html, Web site last accessed September 12, 2012.

n. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3034 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low to medium skill would be able to exploit these vulnerabilities.

MITIGATION

Siemens addresses these issues in a Siemens Security Advisory, SSA-864051, which is available on its Web site.[p]

Siemens provides an update for WinCC 7.0 SP2, which fixes vulnerabilities 1, 3, 4, and 5, and recommends installing the patch. Siemens also recommends users 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 the following:

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

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks:

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

o. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:P/A:P), Web site last visited September 12, 2012.

p. ProductCERT Security Advisories, http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm, Web site last accessed September 12, 2012

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[q] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[r] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click Web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams[s] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[t] for more information on social engineering attacks.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

q. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 12, 2012.

r. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 12, 2012.

s. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed September 12, 2012.

t. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed September 12, 2012.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.