ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-348-01—SIEMENS PROCESSSUITE AND INVENSYS INTOUCH POORLY ENCRYPTED PASSWORD FILE

December 13, 2012

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts Siemens ProcessSuite[a] and Invensys Wonderware InTouch products. Researcher Seth Bromberger of NCI Security, LLC and independent researcher Slade Griffin have identified an insecure password storage vulnerability in both Siemens ProcessSuite and Invensys Wonderware InTouch applications. Siemens states that ProcessSuite is outdated and cannot be updated to match current security requirements; Siemens recommends upgrading to a more recent human-machine interface (HMI). Invensys recommends using Windows integrated security rather than the InTouch security subsystem but has created a new patch to mitigate this vulnerability. Successful exploitation of this vulnerability can allow an attacker to log in to the system as a privileged user and take over the application.

AFFECTED PRODUCTS

The following Siemens ProcessSuite versions are affected:

- All versions of ProcessSuite.

Please note that according to Siemens, ProcessSuite was phased out in 2005 and completely discontinued in 2010. Customers using SIMATIC PCS7 / APACS+ OS are not affected.

The following Invensys Wonderware InTouch versions are affected:

- Wonderware InTouch 2012 R2 and previous.

Wonderware applications that use Windows Integrated security or ArchestrA security are not affected.

a. Siemens Security Advisory SSA-370812, http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-370812.pdf

IMPACT

An attacker with read permissions to the password file can decrypt it and obtain all usernames and passwords, allowing logon as a privileged user and take over the application.

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

BACKGROUND

ProcessSuite is a part of a Distributed Control System "APACS+" from Moore Products Inc., which was acquired by Siemens in 2000. Siemens ProcessSuite is based on Wonderware InTouch V7.11 and uses similar authentication mechanisms. Siemens no longer supports ProcessSuite.

ProcessSuite is deployed across several sectors including manufacturing, oil and gas, chemical, and others. Siemens estimates that these products are used primarily in the United States and Canada.

InTouch is an HMI created by Invensys Wonderware used for designing, building, deploying, and maintaining applications for manufacturing and infrastructure operations.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSECURE PASSWORD STORAGE[b]

User management information including passwords is stored in a reversible format in file "Ps_security.ini" by the affected software. An attacker with read permissions to this local file can obtain the passwords, log in as a privileged user, and potentially affect the availability, integrity, and confidentiality of the system.

b. CWE-326: Inadequate Encryption Strength, http://cwe.mitre.org/data/definitions/326.html, Web site last accessed December 12, 2012.

CVE-2012-4693[c] has been assigned to this vulnerability. A CVSS v2 base score of 4.3 has been assigned; the CVSS vector string is (AV:L/AC:L/Au:S/C:P/I:P/A:P).[d]

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker would need local access to the password file to be able to exploit this vulnerability.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

Systems running ProcessSuite are outdated in many aspects and cannot support the latest recommended security practices. As this software is discontinued, Siemens strongly recommends upgrading to a more recent HMI for APACS+.[a] Further information on migration options to PCS 7 / APACS+ OS along with technical support can be located at the Siemens APACS Web site.[e]

Invensys recommends using Windows integrated security features or migrating the HMI and OS to versions currently supported and then install their security update.[f] Please consult with Wonderware Technical Support[g] for help with the update.

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.

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4693, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

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

e. Siemens APACS Web site, http://www.apacs2020.com . Web site last visited December 12, 2012.

f Invensys Cyber Security Updates, http://iom.invensys.com/EN/Pages/CyberSecurityUpdates.aspx

g Wonderware Technical Support Contacts, http://global.wonderware.com/EN/Pages/WonderwareTechnicalSupportContacts.aspx

- 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.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[h] 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—Targeted Cyber Intrusion Detection and Mitigation Strategies,[i] 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.

ICS-CERT CONTACT

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585

For industrial control systems security information and incident reporting: www.ics-cert.org

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/.

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed December 12, 2011.

i. Target Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed December 12, 2012.

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.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public Web sites. All comments or questions related to this document should be directed to ICS-CERT at
ics-cert@hq.dhs.gov.

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.