SSA-420
ISA Security Compliance Institute — System Security Assurance –
Vulnerability Identification Testing Policy Specification

Version 2.6

December 2014

A. DISCLAIMER

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”) provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SPECIFICATION.

WITHOUT LIMITING THE FOREGOING, ASCI DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THIS SPECIFICATION ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE SPECIFICATION AVAILABLE, ASCI IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS ASCI UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE. ANYONE USING THIS SPECIFICATION SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ASCI OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL,PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SPECIFICATION, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SPECIFICATION OR OTHERWISE ARISING OUT OF THE USE OF THE SPECIFICATION, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS SPECIFICATION, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF ASCI OR ANY SUPPLIER, AND EVEN IF ASCI OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Revision history

version	date	changes
2.4	2014.02.10	Initial version published to http://www.ISASecure.org
2.6	2014.12.10	Editorial changes, including general applicability to any ISASecure product certification

Contents

1 Scope 6
2 Normative references 6
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 7
4 Overview 7
5 VIT policy requirements 7
6 Nessus policy settings 8
6.1 General settings 8
6.2 Credentials tab 9
6.3 Plugins tab 9
6.4 Preferences tab 10

Requirement ISASecure_VIT.R1 – Date of vulnerability feed 7
Requirement ISASecure_VIT.R2 – Nessus server version 8
Requirement ISASecure_VIT.R3 – VIT policy parameters 8
Requirement ISASecure_VIT.R4 – Archive and report VIT policy 8

FOREWORD

This is one of a series of documents that defines ISASecure® certifications for control systems products, which are developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). The current list of documents related to ISASecure certifications can be found on the ISCI web site http://www.ISASecure.org.

1 Scope

This document describes a configuration for testing for the presence of known vulnerabilities in control systems products using the Nessus tool (http://www.tenable.com/products/nessus). This type of testing is a part of the evaluation of products toward ISASecure® certification. For example, it is a part of the SRT (System Robustness Test) element of ISASecure SSA (System Security Assurance) certification, and a part of the ERT (Embedded Device Robustness) element of ISASecure EDSA (Embedded Device Security Assurance) certification. (The SSA and EDSA certification schemes are described in the documents [SSA-100] and [EDSA-100], respectively.) The vulnerability test aspect of ISASecure certification is known as VIT (Vulnerability Identification Testing). This document describes how to configure Nessus to carry out VIT.

In particular, the present document specifies and provides rationale for the configuration of a VIT policy file to be used with the Nessus tool to carry out VIT. The present document describes all parameters configured in the Nessus policy used for VIT. The majority of the parameters are the same for all control systems products. However, there is a set of parameters that include authentication parameters for the product being tested. These parameters must be configured for the specific product prior to the execution of the VIT per guidance provided in this document.

This document specifies the Nessus tool version and date for the Nessus vulnerability feed to be used for testing. The set of targets to be scanned under VIT, and pass/fail criteria for the test, are specified in the 310 series documents for each certification scheme that uses VIT, such as [SSA-310] and [EDSA-310].

2 Normative references

[Nessus UG] *Nessus User Guide*, available at http://www.tenable.com/products/nessus/documentation

3 Definitions and abbreviations

3.1 Definitions

.

3.1.1
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.2
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation

3.2 Abbreviations

The following abbreviations are used in this document. For abbreviations used by Nessus not listed here, see NIST Interagency Report 7581 “System and Network Security Acronyms and Abbreviations,” available at http://csrc.nist.gov/publications/nistir/ir7581/nistir-7581.pdf .

ASCI	Automation Standards Compliance Institute
CWE	Common Weakness Enumeration
EDSA	embedded device security assurance
ERT	embedded device robustness testing
VIT	vulnerability identification test
IACS	industrial automation and control system
ISCI	ISA Security Compliance Institute
SRT	system robustness testing
SSA	system security assurance
WMI	Windows Management Instrumentation

4 Overview

This section summarizes the intent and usage for the VIT policy for ISASecure product certification. This policy defines the types of vulnerabilities included in the Nessus scan that is performed for VIT.

The goal of VIT is to find vulnerabilities of all CWE (Common Weakness Enumeration) categories that are reported in the National Vulnerability Database, in any component of a control system product under test. These categories are listed at http://nvd.nist.gov/cwe.cfm . VIT has been designed to run in a lab environment, and does not incorporate safeguards that would be required if running against a live system.

Most parameters of the VIT policy configuration are the same for all products. The only policy settings that need to be configured specific to the product under test are:

- Credentials settings. Tailoring of this configuration element is always required. Guidance in configuring the credentials settings is provided in 6.2.
- Preferences. Settings for a few preferences may need to be modified due to the presence of technologies not in common use for control systems, as described in 6.4.

Any organization may create a Nessus policy in accordance with this document and use it in a licensed copy of the Tenable Networks Nessus tool.

5 VIT policy requirements

Following are requirements regarding the Nessus policy to be used for performing VIT.

Requirement ISASecure_VIT.R1 – Date of vulnerability feed

VIT SHALL be performed using date filters applied to the Nessus commercial feed of known vulnerability information. The date filters SHALL be set so that all plugins are included in the test, that were modified or published before a date at most one month before the date on the ISASecure certificate for a product that is based upon the test.

Requirement ISASecure_VIT.R2 – Nessus server version

VIT SHALL be performed using either (1) the most recent version of the Nessus server, determined as of the date of the filters applied to the vulnerability feed used for the test or (2) any later version of the Nessus server.

Requirement ISASecure_VIT.R3 – VIT policy parameters

The policy used for VIT SHALL be configured in accordance with Section 6 below, "Nessus policy settings."

Requirement ISASecure_VIT.R4 – Archive and report VIT policy

The policy file used for VIT SHALL be saved and provided as part of the overall certification testing report.

6 Nessus policy settings

Each element of the Nessus user interface for policy creation is addressed in the following sections.

6.1 General settings

The General settings define the policy and configure the scan related operations. There are several types of options that control the scanner behavior. These types are grouped together within the General Settings as different setting types. Other general settings not listed below (if any) shall be set to the Nessus defaults.

NOTE The Nessus setting types and the allocation of general settings among the setting types may vary by Nessus release.

- Name: Set to name of product under test
- Visibility: Set to shared
- Description: Policy for ISASecure VIT– SSA-420 document Version m.n (version of the SSA-420 document)
- Allow Post-Scan Report Editing: Unchecked
- Safe Checks: Unchecked
- Silent Dependencies: Unchecked
- Log Scan Details to Server: Checked
- Stop Host Scan on Disconnect: Checked
- Avoid Sequential Scans: Unchecked
- Consider Unscanned Ports as Closed: Unchecked
- Designate Hosts by their DNS Name: Unchecked
- Reduce Parallel Connections on Congestion: Checked
- Use Kernel Congestion Detection (Linux Only): Checked
- TCP Scan: Checked
- UDP Scan: Checked
- SYN Scan: Unchecked

- SNMP Scan: Checked
- Netstat SSH Scan: Checked
- Netstat WMI Scan: Checked
- Ping Host: Checked
- Port Scan Range: all
- Max Checks Per Host: 5
- Max Hosts Per Scan: 100
- Network Receive Timeout (seconds): 5
- Max Simultaneous TCP Sessions Per Host: 15
- Max Simultaneous TCP Sessions Per Scan: 19

6.2 Credentials tab

The Credentials tab configures the Nessus scanner to use authentication credentials during scanning. By configuring credentials, it allows Nessus to perform a wider variety of checks that result in more accurate scan results. In order to achieve the results necessary for the VIT, credential scanning SHALL be configured. Since credentials are unique to each product, this document is not able to provide detailed settings and they must be configured on a product by product basis. Credential settings are required whether local, workgroup or domain authentication is used for the control system product. In addition to the Nessus settings, there are also required settings on the target computers as well.

There are a maximum of four types of credentials that can be set. The types that are set SHALL correspond to the capabilities of the product under test. For example, for a control system that runs on Microsoft Windows platforms and provides a SSH interface into some of its controllers, the tester SHALL configure Windows Credentials and SSH Settings. The tester may also configure Cleartext protocol settings. When the control system includes Windows based host nodes, those Windows host nodes may require additional configuration to support the Nessus credential scan. In addition, if using Windows hosts and domain authentication, the tester SHALL provide a domain administrator account in the Windows environment to support the VIT. The tester SHALL configure each credential setting at the highest privilege level configured in the control system. These settings are well documented in the Nessus documentation [Nessus UG]. The relevant section is “Creating a New Policy,” in particular the subsection titled “Credentials.”

NOTE Some control systems component products may not support credentials, in which case this sub section does not apply.

6.3 Plugins tab

The Plugins tab configures the Nessus plugins to use during the VIT.

Since new plugins are published regularly for Nessus, the VIT policy file used for a product SHALL also include predefined filters. These filters are set to assure that the same plugins can be used for all executions of VIT related to the ISASecure certification of a specific product, so that VIT test results are reproducible. This is done by using date filters.

The settings for the Plugins tab are as follows:

Plugins:

All plugins SHALL be enabled for VIT.

Filter option:

Set to process all filters.

Two filters are part of the policy:

1) Plugin modification date is earlier than [ISASecure selected date]

2) Plugin publication date is earlier than [ISASecure selected date]

In accordance with ISASecure _VIT.R1, in order to pass certification, the date selected must be within one month (31 days) of the date on the ISASecure product certificate. Since the date of this certificate is unknown when the test is being run, the tester may use the current date, but is not required to use it. Using the current date will provide the highest likelihood that the test policy will ultimately comply with ISASecure_VIT.R1. If achievement of certification appears imminent based on all other criteria, and a product passed VIT using date filters more than a month ago, VIT must be rerun using later date filters.

6.4 Preferences tab

The Preferences tab provides a means for granular control over scan policy settings. These settings can be highly customized on a product by product basis for arbitrary products scanned by Nessus. Many of the preferences are related to policy audits or specific platforms, and since the focus of VIT is vulnerability identification for control systems, these settings will remain unset. Settings SHALL be Nessus defaults except where a value is listed below:

- ADSI settings: Only set if the target works with mobile devices in normal operation.
- Apple Profile Manager API Settings: Only set if the target is an Apple server with iOS devices connected in normal operation.
- Global variable settings:
    - Enable CGI scanning: Checked
    - Thorough tests (slow): Checked
- SMB Registry:
    - Start the registry service during the scan: Checked
    - Enable administrative shares during the scan: Checked
- SMTP settings: Only set if a component of the product under test includes a mail server.
- VMware SOAP API Settings: Only set if a component of the product under test is running on a VMware platform.
- Wake-on-LAN: Only set if Wake-on-LAN is configured on the control system product.
- Web Application Tests Settings:
    - Enable Web Application Tests: Checked
    - Try all HTTP methods: Checked
    - Test Embedded web servers: Checked

BIBLIOGRAPHY

[SSA-100] *ISCI System Security Assurance – ISASecure certification scheme,* as specified at http://www.ISASecure.org

[EDSA-100] *ISCI Embedded Device Security Assurance – ISASecure certification scheme,* as specified at http://www.ISASecure.org

[SSA-310] *ISCI System Security Assurance – Requirements for system robustness testing,* as specified at http://www.ISASecure.org

[EDSA-310] *ISCI Embedded Device Security Assurance – Requirements for embedded device robustness testing,* as specified at http://www.ISASecure.org