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

Version 3.2

August 2019

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, information, 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.

C. OTHER TERMS OF USE

Except as expressly authorized by prior written consent from the Automation Standards Compliance Institute, no material from this document owned, licensed, or controlled by the Automation Standards Compliance Institute may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, except for non-commercial use only, provided that you keep intact all copyright and other proprietary notices. Modification of the materials or use of the materials for any other purpose, such as creating derivative works for commercial use, is a violation of the Automation Standards Compliance Institute's copyright and other proprietary rights.

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
3.2	2019.08.04	Change document title to remove word “policy;” modify definition of term certification level; incorporate non-policy VIT requirements from EDSA-310 for CSA and SSA-310 for SSA; remove requirement to monitor essential functions during VIT

Contents

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 the test tool, procedure, configuration, and pass/fail requirements 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. In particular, it is an element of ISASecure CSA (Component Security Assurance) certification, and of ISASecure SSA (System Security Assurance) certification. (The CSA and SSA certification schemes are described in the documents [CSA-100] and [SSA-100], respectively.) The vulnerability test aspect of ISASecure certification is known as VIT (Vulnerability Identification Testing). It is referred to as VIT-C for component testing toward CSA certification, and as VIT-S for system testing toward SSA certification. This document describes requirements for carrying out both VIT-C and VIT-S.

NOTE Prior versions of this document contained Nessus policy configuration information only. Sections 4, 5, and 8 of the present document version incorporate other VIT requirements previously found in [EDSA-310] and [SSA-310]. Those documents are superseded by the present document.

The goal of VIT is to ensure that a component or system is free from known vulnerabilities whose risk ranking exceeds the risk threshold established for the product, based upon the capability security level for the product certification.

This document covers VIT-C tool and procedure requirements for CSA certifications in section 4, and VIT-S requirements for SSA certifications in section 5. These requirements include test environment set-up, the set of targets to be scanned under VIT, and pass/fail criteria for the test. Subsequent sections apply for both VIT-C and VIT-S. Section 6 specifies the Nessus tool version and date for the Nessus vulnerability feed to be used for testing.

Section 7 specifies and provides rationale for the configuration of a VIT policy file to be used with the Nessus tool to carry out VIT. That section describes all parameters configured in the Nessus policy used for VIT, for ISASecure certification. 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.

Test reporting requirements are found in section 8.

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
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

3.1.2
certification level
capability security level for which conformance is demonstrated by a certification

3.1.3
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.4
component

entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.5
embedded device

special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

3.1.6
host device

general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

NOTE Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

3.1.7
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

3.1.8
network device

device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

NOTE Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

3.1.9
operational mode

one of several states selectable by the user that are mutually exclusive, such that the component must be in exactly one of these states, and where the state determines which component functions are available when the component is in that state, such as functions for configuration, control operations, update of firmware

NOTE Not all components use the concept of operational mode. An operational mode is primarily designed to control the availability of functions on a device rather than to define details about how these functions will operate.

3.1.10
security level

measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

NOTE Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.11
software application

one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

NOTE 1 Software applications typically execute on host devices or embedded devices.

NOTE 2 Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

3.1.12
security zone

grouping of logical or physical assets that share common security requirements

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
CSA	component security assurance
CWE	Common Weakness Enumeration
DCS	distributed control system
EDSA	embedded device security assurance
HMI	human machine interface
IACS	industrial automation and control system
IP	Internet (network layer) protocol
ISCI	ISA Security Compliance Institute
OS	operating system
PC	personal computer
PLC	programmable logic controller
SL-C	security capability level
SSA	system security assurance
VIT-C	vulnerability identification test for components
VIT-S	vulnerability identification test for systems
WMI	Windows Management Instrumentation

4 VIT-C tool and procedure requirements for CSA

4.1 Test configuration

4.1.1 Vulnerability identification testing configuration

The basic vulnerability identification test configuration for a component consists of a PC running Nessus with the ISASecure VIT policy.

Requirement VIT-C.R1 – Vulnerability identification testing tool for components

Vulnerability identification testing SHALL be performed on a component using a PC running the Nessus vulnerability scanner product from Tenable Network Security configured with a policy that meets the ISASecure VIT policy specification in Section 6.

Requirement VIT-C.R2 – Vulnerability identification testing configuration for components

The configuration for the vulnerability identification test for a component SHALL include the following elements:

a) the component under test;

b) a PC running Nessus with the ISASecure VIT policy;

c) authentication credentials for the component being tested, if supported by the component;

d) any internal firewall functions of the component configured as they would be by the end customer; and

e) a wired switched or non-switched network path that connects all of the above components.

4.2 Test procedure

Requirement VIT-C.R3 – Vulnerability identification testing execution for components

For VIT-C, the tester SHALL execute the Nessus VIT policy, which is created in accordance with Section 6, against the component. For embedded device components, VIT SHALL be performed in all operational modes in which the control function is available.

The next requirement takes into account the fact that some components may have several accessible network interfaces.

Requirement VIT-C.R4 – VIT-C coverage of all accessible network interfaces

If the component under test supports multiple accessible network interfaces, the vulnerability identification test SHALL be executed on each accessible network interface, one at a time.

NOTE A list of accessible interfaces is submitted to the certifier by the certification applicant in accordance with [CSA-300].

4.3 Test pass criteria

Requirement VIT-C.R5 – Criteria for "pass vulnerability identification testing" for components

A component under test SHALL pass the vulnerability identification test (VIT-C) if the vulnerabilities found meet the threshold for acceptable risk for the capability security level (SL-C) of the certification. The threshold is defined using the base CVSS score as follows:

- SL-C = 1. All "critical" issues identified are either corrected or the reason for them not being relevant has been documented.
- SL-C = 2. All "critical" and "high" issues identified are either corrected or the reason for them not being relevant has been documented.
- SL-C = 3. All "critical", "high", and "medium" issues identified are either corrected or the reason for them not being relevant has been documented.
- SL-C = 4. All issues identified are either corrected or the reason for them not being relevant has been documented.

NOTE: Vulnerability Risk Factors are categorized as critical, high, medium, low or none by the VIT scanning tool.

5 VIT-S tool and procedure requirements for SSA

5.1 Test configuration

5.1.1 Vulnerability identification testing configuration

The basic vulnerability identification testing configuration for a system consists of a PC running Nessus with the ISASecure VIT policy.

Requirement VIT-S.R6 – Vulnerability identification testing tool for systems

Vulnerability identification testing SHALL be performed on the system using a PC running the Nessus vulnerability scanner product from Tenable Network Security configured with a policy that meets the ISASecure VIT policy specification in Section 6.

Requirement VIT-S.R7 – Vulnerability identification testing configuration for systems

The configuration for vulnerability identification testing SHALL include the following elements:

a) each component in the system that has an IP address;

b) a PC that is located in the same security zone and running Nessus with the ISASecure VIT policy;

c) authentication credentials for the system being tested;

d) firewall functions of the system configured as they would be by the end customer; and

e) a wired switched or non-switched network path that connects all of the above components.

5.2 Test procedure

Requirement VIT-S.R8 – Vulnerability identification testing execution for systems

For VIT-S, the tester SHALL execute the Nessus VIT policy, which is created in accordance with Section 6, against each component of the system with an IP address. For embedded device components of the system, VIT SHALL be performed in all operational modes in which the control function is available.

The next requirement takes into account the fact that some system components may have several accessible network interfaces.

Requirement VIT-S.R9 – VIT-S coverage of all accessible network interfaces

If components of the system under test support multiple accessible network interfaces, the vulnerability identification test SHALL be executed on each accessible network interface, one at a time as follows. Accessible network interfaces for components that have CSA certification need not be tested as part of VIT-S SSA certification testing, if the VIT-C scan performed for that CSA certification is sufficiently current per the requirements of the present document (Section 6).

5.3 Test pass criteria

Requirement VIT-S.R10 – Criteria for "pass vulnerability identification testing" for systems

The system under test SHALL pass the vulnerability identification test (VIT-S) if during scans of each system component, the vulnerabilities found meet the threshold for acceptable risk for the capability security level of the certification. The threshold varies by corresponding capability security level (SL-C) of the security zone for the component, and is defined using the base CVSS score as follows:

- SL-C = 1. All "critical" issues identified are either corrected or the reason for them not being relevant has been documented.

- SL-C = 2. All "critical" and "high" issues identified are either corrected or the reason for them not being relevant has been documented.

- SL-C = 3. All "critical", "high", and "medium" issues identified are either corrected or the reason for them not being relevant has been documented.

- SL-C = 4. All issues identified are either corrected or the reason for them not being relevant has been documented.

NOTE Vulnerability Risk Factors are categorized as critical, high, medium, low or none by the VIT scanning tool.

6 VIT policy requirements for CSA and SSA

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 7.2.
- 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 7.4.

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.

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

Requirement VIT.R11 – 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 VIT.R12 – 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 VIT.R13 – VIT policy parameters

The policy used for VIT SHALL be configured in accordance with Section 7 below, "Nessus policy settings."

7 Nessus policy settings for CSA and SSA

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

7.1 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

7.2 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.

7.3 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 VIT.R11, 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 VIT.R11. 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.

7.4 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

8 VIT reporting requirements for CSA and SSA

This section contains requirements on VIT test reporting. These are in general common to CSA and SSA certifications. The few differences are noted.

Requirement VIT.R14 – VIT report summary

The VIT process SHALL produce a summary report of all results of VIT testing, in addition to providing detailed test results.

Requirement VIT.R15 – Test report administrative information

The VIT process SHALL produce a test report that includes the following information:

- supplier information for the product under evaluation:
  - for components (CSA), the supplier of the component;
  - for systems (SSA), the manufacturers of all components in the system under test;
- the applicant for the certification (typically the product vendor, but this may be another organization that owns the intellectual property associated with the device);
- the testing laboratory and contact information;
- version information for the product under evaluation:
  - for components (CSA), an identifier that specifies the version of the product under test;
  - for systems (SSA), a system product version number that defines the version of all components as well as configuration version of all components in the system under test;
- an identifier of the ISASecure Test Specification version to which the testing conforms;
- version (date code) of test tools;
- date of the test report; and
- pass/fail status.

Requirement VIT.R16 – Report VIT target configuration

The VIT report SHALL describe the test configuration used to conduct the tests, including:

- For components, the configuration of the component under test;
- For systems, the configuration of all components included in the system.

Requirement VIT.R17 – Report ISASecure reference for test failure

For any test outcomes that result in a certification not being granted, the VIT report SHALL reference the applicable requirement(s) or set of related requirements in the ISASecure test specification upon which that test is based.

Requirement VIT.R18 – Report test failure analysis

For any test failures, whether or not they result in a certification not being granted, the VIT report SHALL describe the discussion, analysis and conclusions reached regarding the failure that took place between the test laboratory and the applicant for certification.

Requirement VIT.R19 – Report test software versions

The VIT report SHALL provide full software version identifiers that, taken together with the test laboratory's procedures, unambiguously define the specific test software used to carry out all tests, to support reproducibility of test results.

Requirement VIT.R20 – Report test identification and parameters for reproducibility

The VIT report SHALL provide information sufficient to support the unambiguous reproducibility of all tests, such as a test version and any parameters.

Requirement VIT.R21 – Report vulnerability identification failures

The VIT report SHALL document any Critical, High, Medium or Low Risk Factor vulnerabilities which were identified during vulnerability identification testing. The report shall also specify those vulnerabilities that were corrected, and vulnerabilities not relevant and document the reason for this, for those vulnerabilities with criticality that requires one of these actions in accordance with Requirement VIT-C.R5 (for CSA) or Requirement VIT-S.R10 (for SSA).

Requirement VIT.R22 – Report accessible interface with identified vulnerability

For vulnerability identification tests which had an observed failure, the accessible interface and component that exhibited the vulnerability SHALL be documented.

Requirement VIT.R23 – Archive and report VIT policy

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

BIBLIOGRAPHY

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

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

[SSA-310] *ISCI System Security Assurance – Requirements for system robustness testing,* as archived at http://www.ISASecure.org (Superseded by present document)

[EDSA-310] *ISCI Embedded Device Security Assurance – Requirements for embedded device robustness testing,* as archived at http://www.ISASecure.org (Superseded by present document)