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

Version 4.5

December 2022

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 https://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
4.5	2022.12.15	Update for current non-default Nessus parameter settings, VIT-C.R2 and VIT-S.R7 modified so product under test is configured per supplier hardening guidelines, VIT-C.R1 and VIT.R14 treat case of no accessible network interfaces, VIT-C.R2 and VIT-S.R7 address wireless; VIT-S.R7 refer to reference layout, VIT-C.R3 change control function to essential function, add new section 9 covering case where Nessus does not support platform of a component under evaluation, add Appendix of all Nessus scanning parameters

Contents

List of tables

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 https://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® Vulnerability Scanner (https://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. The component or system that will be the subject for VIT-C or VIT-S respectively, is the component or system that is under evaluation for CSA or SSA certification.

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 Appendix in Section 10 provides detail in support of Section 7. The majority of the policy 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. Section 9 covers the case in which Nessus does not support testing for the platform of a component under evaluation.

2 Normative references

NOTE: Detailed information in the present document corresponds to Nessus 10.1.x. The Section 10 Appendix specifies procedures in the case of future changes to the functionality available in Nessus.

[Nessus UG] *Nessus User Guide*, available at
https://docs.tenable.com/nessus/10_1/Content/GettingStarted.htm

[SSA-300] *ISCI System Security Assurance – ISASecure certification requirements,* as specified at https://www.ISASecure.org

[CSA-303] *ISASecure CSA Sample Report*, available on request to ISCI

[ICSA-303] *ISASecure ICSA Sample Report*, available on request to ISCI

[SSA-303] *ISASecure SSA Sample Report*, available on request to ISCI

3 Definitions and abbreviations

3.1 Definitions

3.1.1
accessible network interface
network interface declared by the certification applicant as suitable for use during operation or maintenance, and such that connection can occur without physical reconfiguration

NOTE Some network interfaces on systems are internal connections only, and/or have physical protection intended to help prevent an unauthorized network connection. These would not be considered to be accessible network interfaces. A list of accessible network interfaces is submitted by the certification application for CSA ([CSA-300] Requirement ISASecure_C.R4) and SSA ([SSA-300] (Requirement ISASecure_SY.R11).

3.1.2
capability security level
level that indicates capability of meeting a security level natively without additional compensating countermeasures when properly configured and integrated

3.1.3
certification level
capability security level for which conformance is demonstrated by a certification

3.1.4
control system
hardware and software components of an IACS

NOTE Control systems include systems that perform monitoring functions.

3.1.5
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

3.1.6
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.

3.1.7
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.).

3.1.8
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

3.1.9
layout
description of a specific instance of a scalable control system, that defines quantities of zones and resident components, and internal and external interfaces

3.1.10
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.

3.1.11
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.

3.1.12
reference layout
specific layout for scalable control system, that represents security characteristics found in any layout to be SSA certified, in a manner suitable to support testing that provides assurance for all such layouts

3.1.13
scalable control system
control system which supports replication of zones and/or components to support small and large installations

3.1.14
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.

3.1.15
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.

3.1.16
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 https://csrc.nist.gov/publications/nistir/ir7581/nistir-7581.pdf.

ASCI	Automation Standards Compliance Institute
CSA	component security assurance
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
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
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
OS	operating system
PC	personal computer
PLC	programmable logic controller
SL-C	capability security 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. If Nessus does not support scanning for the platform of the component, see Section 9.

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

For components with at least one accessible network interface, vulnerability identification testing SHALL be performed on the component by executing scan(s) as specified in this document on that component

[1] [2] using a PC running a licensed version of the Nessus Vulnerability Scanner product from Tenable Network Security where those scans[3] use a policy[4] 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 a scan definition configured to meet the ISASecure VIT policy;

c) component under test configured as described in the guidelines for hardening the product documented by the supplier in accordance with 62443-4-1 requirement SG-3, including for example these elements:

- authentication credentials[5] for the component being tested, if supported by the component;
- where possible and where not prohibited by the hardening guidelines, services present are turned on and ports are opened;
- any internal firewall functions of the component configured as they would be by the end customer; and

d) a stable switched or non-switched IP network path that connects all of the above components, which may be wired or wireless, using a wired connection if available.

4.2 Test procedure

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

For VIT-C, the tester SHALL execute scan(s) on the component under test, using a Nessus VIT policy, which is created in accordance with Section 6. For embedded device components, VIT scans SHALL be performed in all operational modes in which an essential 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, VIT scans 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 (Common Vulnerability Scoring System) 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. If Nessus does not support scanning for the platform of some component of the system, see Section 9.

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

Vulnerability identification testing SHALL be performed on the system by executing scan(s) as specified in this document on that system[1] [2] using a PC running the Nessus Vulnerability Scanner product from Tenable Network Security, where those scans[3] use a policy[4] 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) system components connected per the reference layout submitted for the system per [SSA-300] **Requirement ISASecure_SY.R3 Reference layout**

c) a PC that is located in the same security zone and running Nessus with a scan definition configured to meet the ISASecure VIT policy;

d) system configured as described in the guidelines for hardening the product documented by the supplier in accordance with 62443-4-1 requirement SG-3, including but not limited to these elements:

- authentication credentials[5] for the system being tested;
- where possible and where not prohibited by the hardening guidelines, services present are turned on and ports are opened;
- firewall functions of the system configured as they would be by the end customer; and

e) to connect Nessus to the system components, a switched or non-switched network path that may be wired or wireless, using a wired connection if available.

5.2 Test procedure

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

For VIT-S, the tester SHALL execute scans against each component of the system under test with an IP address, using a Nessus VIT policy, which is created in accordance with Section 6. For embedded device components of the system, VIT scans 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, VIT scans 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 https://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:

- Settings for SMTP, Wake-on-LAN, and an Oracle database, only set if the component supports these features These settings are found on the Settings tab for a Nessus policy. See Table 1 to locate these settings in the Nessus user interface.
- Credentials settings. Tailoring of this configuration element is always required. Guidance in configuring the credentials settings is provided in 7.2. These settings are found on the Credentials tab for a Nessus policy. See Table 2 to locate these settings in the Nessus user interface.

Any organization may create a Nessus policy in accordance with this document and use it in a licensed copy of the Tenable 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[6] 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.

NOTE Further detail on configuration to meet this requirement is provided in Section 7.3.

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 Policy and configuration settings

The Nessus settings in the table below, together with the Appendix in Section 10 of this document, 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 policy areas as different setting types. Other settings not listed below SHALL be set to the Nessus defaults for the Advanced Dynamic Scan template, with exceptions as described in the Appendix. This template SHALL be used to create a VIT scanning policy, as it supports the use of plugins options described in 7.3.

The “Doc” column provides a related link to the Nessus user guide. In general, any constraints that prevent Nessus from completing its scan have been removed when defining this policy.

NOTE: These settings correspond to Nessus 10.1.x. See the Appendix regarding use of later versions of Nessus.

Table 1. Non-default VIT policy settings

.

Policy Area	Name in Nessus 10.1.x	Default Setting	VIT Setting	Doc	Comments
Discovery->Host Discovery -> Fragile Devices	Scan Network Printers	Unchecked/ Disabled	Checked/ Enabled	Link	
Discovery->Host Discovery -> Fragile Devices	Scan Operational Technology devices	Unchecked/ Disabled	Checked/ Enabled	Link	This is an important setting because Nessus will otherwise detect IACS protocols and cease further scanning.
Discovery->Host Discovery-> Wake-on-LAN	List of MAC addresses	None	Per test environment	Link	Only enter addresses if Wake-on-LAN is configured on the control system product.
Discovery -> Port Scanning	Port scan range	Default	all	Link	This is a text field that will say "default" and is to be changed to the word "all" (without quotes).
Discovery->Port Scanning -> Network Port Scanners	TCP	Unchecked/ Disabled	Checked/ Enabled	Link	This option is only available on Linux or FreeBSD, and not when running Nessus on Windows or MAC OS X. Use of any of these platforms is acceptable.

Policy Area	Name in Nessus 10.1.x	Default Setting	VIT Setting	Doc	Comments
Discovery->Port Scanning -> Network Port Scanners	SYN	Unchecked/ Disabled	Checked/ Enabled	Link	
Discovery->Port Scanning->Network Port Scanners	Override Automatic Firewall Detection	Use soft detection radio button	Disable detection radio button.	Link	Available when TCP or SYN is enabled.
Discovery->Port Scanning -> Network Port Scanners	UDP	Unchecked/ Disabled	Checked/ Enabled	Link	
Discovery->Service Discovery	Search for DTLS on	None	All UDP ports		
Assessment -> General	Override normal accuracy	Unchecked/ Disabled, “Avoid potential False alarms”	Checked/ Enabled, “Show potential False alarms”	Link	Set this way because products under test are not released to the public yet, so they may not have known/documented CVEs or version-based vulnerabilities and therefore a more thorough check is warranted even though it may also find false alarms.
Assessment -> General	Perform Thorough Tests	Unchecked/ Disabled	Checked/ Enabled	Link	
Assessment -> General	SMTP	None	Domain and addresses per test environment	Link	Only set if a component of the product under test includes a mail server. It is possible the supplier is not aware that it is present in their product. Results of the Nessus port scan would indicate its presence. Default values for domain and addresses could be used for this testing in that case.
Assessment -> Brute Force	Only use credentials provided by the user	Checked/ Enabled	Unchecked/ Disabled	Link	Verify with the supplier if the component locks out accounts after several invalid attempts. If yes, then leave this setting enabled.
Assessment->Brute Force->Oracle Database	Test default accounts	Unchecked/ Disabled	Checked/ Enabled	Link	Set to Enabled if product contains Oracle database
Assessment -> Web Applications	Scan Web Applications	Off	On	Link	This enables webapp checks.
Assessment -> Web Applications-> Application Test Settings	Follow dynamically generated pages	Unchecked/ Disabled	Checked/ Enabled	Link	

Policy Area	Name in Nessus 10.1.x	Default Setting	VIT Setting	Doc	Comments
Assessment -> Web Applications-> Application Test Settings	Enable generic web application tests	Unchecked/ Disabled	Checked/ Enabled	Link	
Assessment -> Web Applications-> Application Test Settings	Try all HTTP methods	Unchecked/ Disabled	Checked/ Enabled	Link	
Assessment -> Web Applications-> Application Test Settings	Attempt HTTP Parameter Pollution	Unchecked/ Disabled	Checked/ Enabled	Link	
Assessment -> Web Applications-> Application Test Settings	Test embedded web servers	Unchecked/ Disabled	Checked/ Enabled	Link	
Assessment -> Web Applications-> Application Test Settings	Do not stop after first flaw is found per web page	Unchecked/ Disabled	Checked/ Enabled, "Look for all flaws (slowest)"	Link	
Report -> Processing	Override normal verbosity	Unchecked/ Disabled	Checked/ Enabled, “Report as much information as possible”	Link	
Report -> Processing	Hide results from plugins initiated as a dependency	Checked/ Enabled	Unchecked/ Disabled	Link	
Report -> Output	Allow users to edit scan results	Checked/ Enabled	Unchecked/ Disabled	Link	
Report -> Output	Display hosts that respond to ping	Unchecked/ Disabled	Checked/ Enabled	Link	
Advanced -> General Settings	Enable safe checks	Checked/ Enabled	Unchecked/ Disabled	Link	
Advanced -> General Settings	Stop scanning hosts that become unresponsive during the scan	Unchecked/ Disabled	Checked/ Enabled	Link	
Advanced-> Performance Options	Slow down the scan when network congestion is detected	Unchecked/ Disabled	Checked/ Enabled	Link	Disabling could degrade quality of scan.
Advanced -> Performance Options	Network timeout (in seconds)	5	15	Link	Policy increases the timeout to reduce the likelihood of missing a finding due to timeout.
Advanced -> Debug Settings	Log scan details	Unchecked/ Disabled	Checked/ Enabled	Link	

7.2 Credentials page

The Credentials page for a scan policy 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.

The types of credentials 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.

Credential settings are well documented in the Nessus documentation [Nessus UG]. The relevant section is "Scans->Scan and Policy Templates," in particular the subsection titled "Credentials." Further information about configuring testing for Windows and for SSH login to Linux systems is provided in the sections in Nessus user guide titled "Credentialed checks on Windows" and "Credentialed checks on Linux."

The certifier SHALL examine all credential options to determine if they are applicable to the product being scanned. The following have been identified as relevant for some IACS components; however, others may be relevant as well to a component under evaluation.

Table 2. Credentials settings that may be relevant

Policy Area	Name in Nessus 10.1.x	Default Setting	VIT Setting	Docs	Comments
Credentials -> Host->Windows - Global Credential Settings	Start the Remote Registry service during the scan	Unchecked/ Disabled	Checked/ Enabled	Link	If adding a Windows Host credential, enable this setting to ensure a thorough and complete credentialed scan.
Credentials ->Host-> Windows - Global Credential Settings	Enable Administrative shares during the scan	Unchecked/ Disabled	Checked/ Enabled	Link	If adding a Windows Host credential, enable this setting to ensure a thorough and complete credentialed scan.
Credentials-> Host->SSH	Attempt least privilege	Unchecked/ Disabled	Checked/ Enabled	Link	If adding credentials for SSH login such as to a Linux host or network device, enable this setting to determine the level of privilege needed to exploit particular vulnerabilities.
Credentials -> Miscellaneous	ADSI	None	Per test environment	Link	Only set if the target works with mobile devices in normal operation.
Credentials -> Miscellaneous	VMware ESX SOAP API	None	Per test environment	Link	Only set if a component of the product under test is running on a VMware platform.

Policy Area	Name in Nessus 10.1.x	Default Setting	VIT Setting	Docs	Comments
Credentials -> Miscellaneous	VMware vCenter SOAP API	None	Per test environment	Link	Only set if a component of the product under test is running VMware vCenter.

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

7.3 Plugins options

The Plugins options for an advanced dynamic scan configure the Nessus plugins to use during the VIT. See the Nessus user guide section titled "Configure dynamic plugins."

Since new plugins are published regularly for Nessus, the VIT policy file used for a product SHALL also include predefined filters using the Dynamic Plugins feature, set using the Dynamic plugins tab of a policy. 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 options 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) The plugin attribute "Plugin modification date" is earlier than [ISASecure selected date]

2) The plugin attribute "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.

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.

VIT reports use information from reports created by Nessus, and add additional information.

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. If no testing is performed because the product has no accessible network interfaces, it will be sufficient for the overall certification report to record this fact and rationale in its section on VIT.

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 component or system);
- 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.

9 Platform not supported by Nessus

Requirement VIT.R24 – VIT when no Nessus support for component platform

If a component under evaluation or a component of a system under evaluation, is based on a platform not supported by Nessus, the certifier SHALL perform one of, or a combination of, the following actions in place of running a Nessus scan for VIT.

- Perform a manual analysis to find known vulnerabilities for the component, based on the bill of materials for the component and the CVE (Common Vulnerabilities and Exposures) database.
- Witness the supplier running a known vulnerability test on their product. In this case, the date of this test SHALL be at most 30 days before the date to appear on the certificate. The target component for the test SHALL be configured in accordance with the security guidelines for the product, with no additional features enabled or additional countermeasures used.
- Perform certifier testing using the known vulnerability testing tool that the supplier has used for this type of testing in their development process, following all applicable requirements in the present document.

Passing VIT SHALL be determined in accordance with the CVSS score threshold described in Requirement VIT-C.R5 for components and Requirement VIT-S.R10 for systems, where such a component is a part of that system.

NOTE It is a separate criterion under the Security Development Artifacts (SDA) element of a CSA or SSA certification, for verifying compliance to IEC 62443-4-1 requirement SVV-3, that the supplier performs black box known vulnerability testing as part of their software development process. Therefore a supplier to pass certification will have identified or created a tool that supports the platform for their product.

Requirement VIT.R25 – Supplier VIT reporting when no Nessus support for component platform

In the case that the certifier witnesses the supplier's black box known vulnerability testing in accordance with Requirement VIT.R24, the supplier SHALL provide a report to the certifier that SHOULD meet the following requirements in Section 8 of this specification: Requirements VIT.R15-R16, Requirements VIT.R19-R23. However, "policy file" in Requirement VIT.R23 MAY be replaced by an alternative method of archiving testing parameters.

Requirement VIT.R26 – Certifier VIT reporting when no Nessus support for component platform

In the case that the certifier carries out a manual database search for known vulnerabilities in accordance with Requirement VIT.R24, the certifier SHALL create a detailed VIT report that describes the dates and parameters

of searches performed, and provides analysis information for vulnerabilities found as described under Requirements VIT.R14, R17, R18 and R21.

In the case that the certifier performs or witnesses testing using the supplier's black box known vulnerability testing tool in accordance with Requirement VIT.R24, the certifier SHALL create a detailed VIT report that meets the requirements of Section 8 of this document. However, "policy file" in Requirement VIT.R23 MAY be replaced by an alternative method of archiving testing parameters. In the case of witnessing, the report MAY meet the requirements of Section 8 using references to the supplier's VIT report submitted under Requirement VIT.R25. In either case the certifier SHALL provide the analysis information described under Requirement VIT.R17 and Requirement VIT.R18.

If there is no Nessus support for a component platform, the overall certification report provided by the certifier that uses the ISASecure report template (specification ID "303"), SHALL include the following information in the VIT section of that report:

- Nessus does not support the platform of component(s) under evaluation, providing identifiers for component(s) and unsupported platforms
- Therefore assessment of known vulnerabilities was carried out using an alternative process specified by the ISASecure program: <describe action(s) taken under Requirement VIT.R24>.
- Results of the assessment performed, which SHOULD use the format provided by the 303 template for VIT report section.

10 Appendix – Nessus Policy Settings Detail

This appendix lists all Nessus 10.1.x policy settings and values to be used to perform Nessus scans for ISASecure VIT-C and VIT-S. All policy settings other than those specified in 7.1 and 7.2 of the present document, SHALL be set to Nessus defaults, except where a value is noted below to be set at the discretion of the responsible chartered laboratory. In these cases, any setting may be used.

Requirement VIT.R12 of the present document, specifies the version of Nessus to be used for VIT-C and VIT-S. It is possible that a version later than Nessus 10.1.x may be used, while the present version of the SSA-420 document remains valid for ISASecure certification. It is the intent to provide any required updates to these specification settings. In any interim period until such updates are available, the specifications for settings in the current document are to be applied as follows for Nessus versions later than 10.1.x.

If a Nessus default value changes from that used for Nessus 10.1.x, in a Nessus version later than 10.1.x that is used for VIT, the value specified in the present document together with SSA-420 errata adopted by the ISCI Governing Board, SHALL be used.

If additional policy settings are introduced in Nessus versions after 10.1.x, the value for any setting not in the list below SHALL be set at the discretion of the chartered laboratory responsible for the VIT evaluation, by considering its relevance to the product under evaluation.

Bold italic font in the lists below designates a group of several settings to be customized for the product under evaluation, as opposed to a single setting, which is shown in **non-italic bold font**.

- ***Basic Settings for Policies*** – naming and permissions on policies, values at discretion of chartered laboratory
- Discovery Settings
    - Host Discovery
        - General Settings
            - **Ping the remote host** Default On, which is recommended for troubleshooting purposes but may be set at the discretion of the chartered laboratory. When scanning a specific device IP that you know is online, you may decide to disable this since it gives no further information, and not all devices may reply to ping.

- **Test the local Nessus host** – Default Enabled, but setting not relevant if local Nessus host itself is not in range of scan, and therefore at discretion of chartered laboratory in that case
- **Use Fast Network Discovery** – Default Disabled, but setting not relevant assuming *Ping the remote host* is OFF, and therefore at discretion of chartered laboratory in that case

▪ ***Ping Methods*** – Settings not relevant if *Ping the remote host* is OFF, or if specific setting is not relevant for the component, and therefore the following are set at the discretion of chartered laboratory in that case as they will have no effect. If *Ping the remote host* is ON, those values to be used for settings relevant to the component are set as follows:
- **ARP** – Default Enabled
- **TCP** – Default Enabled
- **Destination ports (TCP)** – Default built-in
- **ICMP** – Default Enabled
- **Assume ICMP unreachable from the gateway means the host is down** – Default Disabled
- **Maximum number of retries** – Default 2
- **UDP** – Default Disabled

▪ Fragile Devices
- **Scan network printers** – specified in Section 7.1
- **Scan Novell Netware Hosts** – Default Disabled
- **Scan operational technology devices** –specified in Section 7.1

▪ Wake-on-LAN
- **List of MAC addresses** – specified in Section 7.1
- **Boot time wait** – Default 5 minutes

o Port Scanning
▪ Ports
- **Consider unscanned ports as closed** – Default Disabled
- **Port scan range**-specified in Section 7.1

▪ Local Port Enumerators
- **SSH**-Default Enabled
- **WMI** – Default Enabled
- **SNMP** – Default Enabled
- **Only run network port scanners if local port enumeration failed** – Default Enabled
- **Verify local TCP ports found by local port enumerators** – Default Disabled

▪ Network Port Scanners
- **TCP**- specified in Section 7.1
- **SYN**- specified in Section 7.1
- **Override automatic firewall detection** - specified in Section 7.1
- **UDP**- specified in Section 7.1

o Service Discovery
▪ General Settings
- **Probe all ports to find services** – Default Enabled
- **Search for SSL based services** – Default On

▪ Search for SSL/TLS Services
- **Search for SSL/TLS on** – Default Known SSL/TLS ports
- **Search for DTLS on** – specified in Section 7.1
- **Identify certificates expiring within x days** – Default 60
- **Enumerate all SSL ciphers** – Default True

- **Enable CRL checking** – Default False

- Assessment Settings
  - General
    - Accuracy
      - **Override normal Accuracy** – specified in Section 7.1
      - **Perform thorough tests** – specified in Section 7.1
    - Antivirus
      - **Antivirus definition grace period** (days) – Default 0
    - SMTP
      - **Third party domain** – specified in Section 7.1
      - **From address** – specified in Section 7.1
      - **To address** – specified in Section 7.1
  - Brute Force
    - General Settings
      - **Use only credentials provided by the user** – specified in Section 7.1
    - Oracle Database
      - **Test default accounts** – specified in Section 7.1
    - ***Hydra*** – These settings should not be visible. Hydra is not used for VIT and shall not be installed on the Nessus host. The settings only appear in Nessus if Hydra is installed on the Nessus host.
  - SCADA
    - Modbus TCP Coil Access
      - **Start at Register** – Default 0
      - **End at Register** – Default 16
    - ICCP/COTP TSAP Addressing Weaknesses
      - **Start COTP/TSAP** – Default 8
      - **Stop COTP/TSAP** – Default 8
  - Web Applications
      - **Scan web applications** – specified in Section 7.1 (and in this case the following settings, through “Application Test Settings,” are offered)
    - General Settings
      - **Use a custom User-Agent** – Default Mozilla/4.0
    - Web Crawler
      - **Start crawling from** – Default /
      - **Excluded pages (regex)** – Default - /server_privileges\.php <> log out
      - **Maximum pages to crawl** – Default 1000
      - **Maximum depth to crawl** – Default 6
      - **Follow dynamically generated pages** – specified in Section 7.1
    - Application Test Settings
      - **Enable generic web application tests** – specified in Section 7.1
      - **Abort web application tests if HTTP login fails** – Default Disabled
      - **Try all HTTP methods** – specified in Section 7.1
      - **Attempt HTTP Parameter Pollution** – Specified in Section 7.1
      - **Test embedded web servers –** specified in Section 7.1
      - **Test more than one parameter at a time per form –** Default Disabled
      - **Do not stop after first flaw is found per web page** – specified in Section 7.1
      - **URL for Remote File Inclusion** – Default http://rfi.nessus.org/rfi.txt, or use local copy of this file at discretion of the chartered laboratory
      - **Maximum run time (min)** – Default 5

- Windows
  - General Settings
    - **Request information about the SMB domain** – Default Disabled
  - User Enumeration Methods
    - **SAM Registry** – Default Enabled
    - **ADSI Query** – Default Enabled
    - **WMI Query** – Default Enabled
    - **RID Brute Forcing** – Default Disabled
- Malware
  - General Settings
    - **Disable DNS resolution** – Default Disabled
  - Hash and Allowlist Files
    - **Custom Netstat IP Threat List** – Default None
    - **Provide your own list of known bad MD5 hashes** – Default None
    - **Provide your own list of known good MD5 hashes** – Default None
    - **Hosts file allowlist** – Default None
    - **Yara Rules** – Default None
  - File System Scanning
    - **Scan file system** – Default Off
- Databases
  - Oracle database
    - **Use detected SIDs** – Default Disabled

- Report Settings
  - Processing
    - **Override normal verbosity** – specified in Section 7.1
    - **Show missing patches that have been superseded** – Default Enabled
    - **Hide results from plugins initiated as a dependency** – specified in Section 7.1
  - Output
    - **Allow users to edit scan results** – specified in Section 7.1
    - **Designate hosts by their DNS name** – Default Disabled
    - **Display hosts that respond to ping** – specified in Section 7.1
    - **Display unreachable hosts** – Default Disabled
    - **Display Unicode characters** – Default Disabled
- Advanced Settings
  - General Settings
    - **Enable Safe Checks** – specified in Section 7.1
    - **Stop scanning hosts that become unresponsive during the scan** – specified in Section 7.1
    - **Scan IP addresses in a random order** – Default Disabled
    - **Automatically accept detected SSH disclaimer prompts** – Default Disabled
    - **Scan targets with multiple domain names in parallel** – Default Disabled
    - **Create unique identifier on hosts scanned using credentials** – Default Enabled (feature not used in Nessus Vulnerability Scanner, so set at discretion of chartered laboratory)
  - Performance
    - **Slow down the scan when network congestion is detected** – specified in Section 7.1
    - **Network timeout (in seconds)** – specified in Section 7.1
    - **Max simultaneous checks per host** – Default 5
    - **Max simultaneous hosts per scan** – Default smaller of 30 or Nessus default global value based on the hardware running Nessus

        - **Max number of concurrent TCP sessions per host** – Default None, set at discretion of chartered laboratory to clear possible reported connections refused
        - **Max number of concurrent TCP sessions per scan** – Default None, set at discretion of chartered laboratory to clear possible reported connections refused
        - ***Unix find command exclusions*** – Default all of these to None
    - Debug Settings
        - **Log scan details** – specified in Section 7.1
        - **Enable plugin debugging** – Default Disabled. Set to either Disabled or Enabled.
        - **Audit Trail Verbosity** – Default Default (Full)
        - **Include the KB** – Default Default
        - **Enumerate launched plugins** – Default Disabled. Set to either Disabled or Enabled
- Credentials settings – Section 7.2 of this document specifies that all available Credential settings are to be customized based upon features of the product under evaluation, and specifies a few specific Windows Global Credentials settings (if relevant). Only the Global Credential Settings related to Windows and SSH are listed here.
    - Host
        - ***Secure Shell (SSH)*** If these are set, also use the Global Credential Settings following.
            - Global Credential Settings
                - **known_hosts file** – Default none
                - **Preferred port** – Default 22, at discretion of chartered lab to reset if a different port is used
                - **Client version** – Default OpenSSH_5.0
                - **Attempt least privilege** – specified in 7.2
        - ***Windows*** – If these are set, also use Global Credential Settings following.
            - Global Credential Settings
                - **Never send credentials in the clear** - Default Enabled
                - **Do not use NTLMv1 authentication** – Default Enabled
                - **Start the Remote Registry service during the scan** – specified in 7.2
                - **Enable administrative shares during the scan** – specified in 7.2
                - **Start the Server service during the scan** – Default Disabled

BIBLIOGRAPHY

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

[CSA-300] *ISCI Component Security Assurance – ISASecure certification requirements,* as specified at https://www.ISASecure.org

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

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

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

[1] The following notes refer to the user interface in Nessus Vulnerability Scanner 10.1.x.

[2] Run a scan under Scans->MyScans, by clicking the launch icon for the selected scan.

[3] Create a scan based upon a policy by selecting that policy under Scans->User Defined.

[4] Create a policy for VIT under Scans->Policies->New Policy->Advanced Dynamic Scan Template.

[5] Set authentication credentials under Scans->Policies->New Policy->Advanced Dynamic Scan Template->Credentials.

[6] Date filters for a policy are set under Scans->MyScans->Policies, by selecting the policy to edit, clicking on More, clicking on Configure, and then using the Dynamic Plugins tab. Date filters are available for policies created using the Advanced Dynamic Plugins template, which is used for VIT.