VMware Security Technical Implementation Guide (STIG) Program Overview

vmware

Table of contents

Overview

VMware is a trusted partner in highly secure, mission critical systems around the world, including the US Department of Defense (DoD). In the DoD, all IT systems must adhere to the rigorous Risk Management Framework (RMF) as defined in DoDI 8510.01. A critical component of RMF is the mandatory implementation of Security Technical Implementation Guides (STIGs) and Security Requirements Guidelines (SRGs) as maintained by the Defense Information Systems Agency (DISA).

To serve our customers in the DoD and others who wish to meet the bar set by the DoD, VMware actively engages with DISA to produce and publish STIGs through their vendor STIG development process.

What is a STIG/SRG?

First let's look at how these terms are defined in DoDI 8510.01 as follows:

"STIGs are product-specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 security controls into single, actionable, measurable items. SRGs are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used."

A STIG in our terms is a product specific hardening guide based on security requirements from the DoD that contains detailed and comprehensive steps to audit and remediate the requirements that have actionable configurations associated with them.

An SRG on the other hand, is a collection of requirements applicable to a given technology family, product category, or organization in general. They are non-product specific requirements used to mitigate common security vulnerabilities encountered across information technology systems and applications.

SRGs are the source documents developed by DISA from which a STIG is derived. SRGs come in a number of broad categories such as "Web Server" and "Database". The process of creating a STIG is largely determining what SRG(s) apply to a product and addressing those requirements.

Official STIGs vs. STIG Readiness Guides

Official STIGs are published by DISA on public.cyber.mil. VMware products must go through the vendor STIG development process mentioned previously to have an official STIG published.

In many instances, even though there may be customer demand for STIG content for a product well before the STIG development process completes, due to resourcing or time constraints, the STIG publication may not happen at all. In some of these cases VMware may make available what we call a "STIG Readiness Guide". This means that we are performing the same level of work as we would normally do with DISA but are self-publishing the content to make it available and usable as soon as possible. The quality is high enough, in our experience, that should a given "STIG Ready" product be put through the DISA process, we are confident that there would be minimal content changes before publication.

These guides represent VMware's effort to document our compliance against the SRG requirements and nothing more. A published STIG is our eventual goal, in most cases, but this content should not be viewed to be "as good as a STIG". A DISA published STIG includes technical validation, review of requirement fulfillment, accuracy and style, risk acceptance and is digitally signed by the DISA Risk Management Executive. Except for products that already have published STIGs, there is no explicit or implied DISA approval of the provided content other than the guidance allows for such content to be used in the absence of an official STIG. We also make no guarantee that any STIG(s) will be published from this content in the future.

STIG Readiness Guides

We are often asked by our DoD customers if our STIG Readiness Guides can be used? The answer is yes.

In the absence of a STIG a DoD customer must fall back to SRGs to harden their environments as written in DoDI 8510.01. "*When a STIG is not available for a product, an SRG may be used."*

For a customer this is often a daunting task to figure out how these generic requirements are met for products with often very little documentation available to aid in the research.

DISA elaborates on this issue for us further in their FAQ here: https://public.cyber.mil/stigs/faqs/#toggle-id-11

"***What do I use if there is no STIG?***

Determine if a STIG has been published for an earlier version of the same product. Many checks and fixes in earlier versions of STIGs can be applied to the new version of the product. If a STIG for an older version of the product is available, review the check and fix procedures to determine which of these work with the new product version. Where possible, use the checks and fixes that work directly with the new version. The remainder of checks and fixes that no longer work with the new product version will need to be evaluated and proper check and fix procedures will need to be determined for each requirement. New product features and configuration settings must also be accounted for based on the relevant SRG.

If there is no related STIG, the most relevant SRG can be used to determine compliance with DoD policies. If assistance is needed in determining which SRG applies to the product, please open a ticket with the STIG Customer Support Helpdesk at disa.stig_spt@mail.mil

In fulfilling a requirement, be it from an SRG or an earlier version of a STIG, ***vendor documentation*** *may be followed for configuration guidance.*"

Using this information, we are able to provide STIG Readiness Guides for use in order to alleviate the burden of trying to carry old STIGs forward to newer product versions or analyzing SRGs.

Support

More information on support for STIGs and STIG Readiness Guides is available in the following KB article: https://kb.vmware.com/s/article/94398

Other Considerations

It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations as such ensure all steps are taken to back systems up before implementation.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. Furthermore, VMware implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is intended for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level because some of the settings may not be able to be configured in environments outside the DoD architecture.

Frequently Asked Questions

What do the severity codes mean?

As stated in the DISA Security Requirements Guides:

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

DISA Category Code Guidelines	
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

Most of the severity codes in the associated guides are CAT IIs. During STIG development DISA may modify severity codes on a per product and context specific basis.

Can I import the XCCDF files into STIG Viewer?

Yes, the XCCDF files can be imported into STIG Viewer and then used to create STIG Checklists as necessary. They can alternatively be viewed by opening the XML file in Internet Explorer.

Are there any scripts or tools to help audit and remediate these controls?

Yes, there are example scripts and playbooks to aid in these tasks available in the GitHub repo linked below. Please carefully examine and test before running these in a production environment.

https://github.com/vmware/dod-compliance-and-automation/

What requirements were considered when developing this content?

All technical NIST SP 800-53 requirements and applicable SRGs were considered while developing this content. Requirements that are applicable and configurable will be included in the final content.