MICROSOFT WINDOWS PRIVILEGED ACCESS WORKSTATION (PAW) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 2

31 May 2022

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

1. INTRODUCTION

1.1 Executive Summary

The Microsoft Windows Privileged Access Workstation (PAW) Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems[1]. This document is meant for use in conjunction with the appropriate version of the Windows STIG.

The Windows PAW STIG provides configuration and installation requirements for dedicated Windows workstations used exclusively for remote administrative management of designated high-value IT resources, including servers, workstations, directory services, applications, databases, and network components. A high-value IT resource is defined as any IT resource whose purpose is considered critical to the organization or whose loss or compromise would cause a significant impact on the organization. The following topics are not in scope for this STIG:

- Rules for setting up and managing privileged accounts (roles, least privilege, etc.)
- Rules for monitoring privileged accounts
- Rules for user account restrictions on IT resources (functions restricted to only privileged account users on IT resources)
- Requirements related to when and how an Authorizing Official (AO) determines which IT resources are designated as "high value"

Microsoft's PAW paper (https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/privileged-access-workstations) was a key reference used during the development of this STIG. It is recommended that system administrators review the paper as they plan the rollout of site PAWs.

This STIG assumes the applicable Windows STIG has been applied to the PAW prior to the implementation of the technical controls listed in this STIG. Note that some configurations required by this STIG may need to be implemented in the domain rather than on the PAW. In addition, and similar to the Microsoft PAW paper, this STIG focuses on the setup and configuration of a PAW on a workstation rather than the setup of multiple PAWs in a VM environment. There are only two requirements in this STIG related to deploying PAWs in a VM environment. If one or more PAWs are installed as virtual machines (VMs) on a host server, this STIG assumes the applicable VM product STIG has been applied. The Microsoft paper is expected to be updated in the future to provide new VM deployment guidance, and an update to this STIG will follow with similar VM deployment information.

---

[1] The scope of this STIG is unclassified systems and networks, but the concepts are also valid for classified systems and networks.

See information on the Microsoft Tier model at https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material. Administrators of high-value IT assets have no administrator rights on the PAW itself.

1.2   Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3   Vulnerability Severity Category Code Definitions

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.

Table 1-1: Vulnerability Severity Category Code Definitions

	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.

1.4   STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5   Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6   Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. 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.

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. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided 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 due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.7   Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF).

DoD AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11

- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards

- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04